

Opis przedmiotu zamówienia

Wymagania techniczne i funkcjonalne dla infrastruktury IT i OT Gminy Jasieniec

Spis treści

I. Macierz do serwerowni	2
II. Kompleksowa platforma cyberbezpieczeństwa klasy EPP/EDR z modułem CTEM	4
III. Oprogramowanie do centralnego zarządzania infrastrukturą IT i stacjami roboczymi	20
IV. Rozwiązanie klasy UTM do segmentacji sieci i VPN do serwerowni	34
V. Wysokowydajny system deduplikacji danych na potrzeby kopii zapasowych zintegrowany z dedykowanym oprogramowaniem do backupu	47
VI. Serwer z oprogramowaniem 2 sztuki	49
VII. UPS do SUW i serwerowni	61
VIII. Switche zarządzalne do SUW i serwerowni	63
IX. Szafa Rack	65
X. Agregat stacjonarny (20 kW) do SUW	67
XI. System monitorowania sieci OT / IDS dla OT	67

Warunki ogólne

1. Zamawiający wymaga przedłożenia kart katalogowych oferowanych rozwiązań lub innych dokumentów udowadniających spełnianie zapisów Opisu Przedmiotu Zamówienia przez zaoferowane rozwiązanie
2. Wszystkie oferowane przez Wykonawcę urządzenia i sprzęt muszą być fabrycznie nowe (wyprodukowane w 2026 roku) oraz pochodzić z oficjalnych kanałów dystrybucyjnych dostępnych na terenie Polski. Dotyczy to również oprogramowania, które musi być dostarczone z autoryzowanych źródeł działających na rynku krajowym.
3. Wykonawca zobowiązany jest do zapewnienia transportu przedmiotu zamówienia, a koszt tej usługi musi być uwzględniony w złożonej ofercie. Odpady opakowaniowe (kartony, folie, papier) zostaną usunięte przez Zamawiającego we własnym zakresie.
4. W przypadku niekompletnych informacji na temat spełniania wymogów Opisu Przedmiotu Zamówienia przez dane rozwiązanie Zamawiający może wezwać oferenta do przedłożenia bardziej szczegółowych informacji, a jeśli te nie będą wystarczające może odrzucić ofertę.
5. Usługa wdrożenia musi być przeprowadzona przez firmę posiadającą minimum dwóch certyfikowanych inżynierów certyfikowanych przez producenta rozwiązania w zakresie dostarczanych serwerów.
6. Zamawiający wymaga odbycia wizji lokalnej przed złożeniem oferty. Wizja lokalna jest niezbędna z uwagi na konieczność zapoznania się z istniejącą infrastrukturą teleinformatyczną, warunkami technicznymi instalacji oraz zakresem prac wdrożeniowych mającymi wpływ na kalkulację ceny oferty. Nieodbycie wizji lokalnej będzie skutkować odrzuceniem oferty.

I. Macierz do serwerowni - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Sieciowa macierz dyskowa (NAS) w obudowie serwerowej do montażu w szafie RACK 19" o wysokości 1U, z 4 zatokami na dyski 3.5". 2. Urządzenie dostarczone wraz z 4 dyskami twardymi 8TB zainstalowanymi w zatokach, gotowe do konfiguracji.
Obudowa	3. Montaż w szafie RACK 19", wysokość 1U, głębokość nie większa niż 500 mm (wymiary maks. 44 × 439 × 499 mm). 4. Zatoki dyskowe wymienne podczas pracy urządzenia (hot-swap), bez konieczności wyłączenia systemu. 5. Wskaźniki LED stanu dysków, urządzenia, sieci oraz rozbudowy pamięci masowej, przyciski zasilania i restartu.
Zasilanie	6. Redundantny zasilacz (dwa moduły zasilające) zapewniający ciągłość pracy w przypadku awarii jednego z zasilaczy. 7. Zasilacze zintegrowane z obudową, zasilanie z sieci 230 V AC / 50 Hz, kable zasilające w zestawie.
Procesor	8. 64-bitowy procesor ARM, 4 rdzenie, taktowanie min. 1,7 GHz, z jednostką zmiennoprzecinkową oraz sprzętowym silnikiem szyfrowania.

Parametr	Charakterystyka (wymagania minimalne)
Pamięć RAM	9. Min. 2 GB DDR4 UDIMM zainstalowane fabrycznie. 10. Możliwość rozbudowy pamięci do min. 16 GB (1 gniazdo UDIMM DDR4). 11. Pamięć Flash min. 512 MB z ochroną systemu operacyjnego typu dual boot.
Dyski twarde	12. 4 × dysk twardy 8 TB, 3.5", interfejs SATA III 6 Gb/s, zainstalowane w urządzeniu. 13. Dyski przeznaczone do pracy w macierzach NAS w trybie 24/7, w wielozatokowych środowiskach RAID, z mechanizmem kontroli błędów odczytu/zapisu dla RAID (typu TLER/ERC). 14. Prędkość obrotowa 7200 obr./min, pamięć podręczna min. 256 MB, technologia zapisu CMR. 15. Obciążalność roczna min. 550 TB/rok, współczynnik MTBF min. 1 000 000 godzin. 16. Czujnik wstrząsów / ochrona przed wibracjami w środowisku wielodyskowym. 17. Dyski z gwarancją producenta min. 5 lat. 18. Dyski pochodzące z oficjalnej listy kompatybilności producenta macierzy.
Obsługiwane nośniki	19. Zatoki 3.5" z obsługą dysków HDD 3.5", HDD 2.5" oraz SSD 2.5" SATA 6 Gb/s / 3 Gb/s. 20. Obsługa pamięci podręcznej SSD (SSD cache) – opcjonalnie przez kartę w gnieździe PCIe.
Konfiguracja RAID i dane	21. Obsługa poziomów RAID 0, 1, 5, 6, 10 oraz JBOD. 22. Obsługa migawek (snapshots) i replikacji danych, kopii zapasowych oraz synchronizacji plików. 23. Obsługa protokołów plikowych i blokowych, w tym SMB/CIFS, NFS, FTP oraz iSCSI; kompatybilność z Windows, macOS i Linux/UNIX. 24. Obsługa Jumbo Frame.
Interfejsy sieciowe	25. Min. 2 porty 10 GbE SFP+. 26. Min. 2 porty 2.5 GbE RJ-45 (2.5G/1G/100M/10M). 27. Obsługa Wake on LAN (WOL) na portach 2.5 GbE.
Gniazda rozszerzeń i porty	28. Min. 1 gniazdo PCIe Gen 2 x2 umożliwiające instalację karty rozszerzeń (np. karty sieciowej, adaptera M.2 SSD). 29. Porty USB 3.2 Gen 1 – min. 2 szt.
Bezpieczeństwo	30. Szyfrowanie woluminów AES 256-bit ze sprzętowym wsparciem silnika szyfrowania. 31. Zabezpieczenie systemu operacyjnego przed uszkodzeniem (dual boot). 32. Obsługa uwierzytelniania i kontroli dostępu użytkowników oraz uprawnień do folderów.

Parametr	Charakterystyka (wymagania minimalne)
Zarządzanie	33. Zarządzanie przez przeglądarkę internetową oraz dedykowaną aplikację producenta, bez konieczności instalacji dodatkowego oprogramowania. 34. Monitorowanie stanu dysków (S.M.A.R.T.), zasilania, temperatury i wentylatorów oraz powiadomienia o zdarzeniach (e-mail, SNMP). 35. Możliwość zarządzania zewnętrznymi urządzeniami RAID tego samego producenta.
Elementy montażowe	36. Komplet szyn montażowych do szafy RACK 19" w zestawie.
Gwarancja	37. Gwarancja producenta na urządzenie zgodnie z warunkami producenta. 38. Gwarancja na dyski twarde min. 5 lat.

II. Kompleksowa platforma cyberbezpieczeństwa klasy EPP/EDR z modułem CTEM

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

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

Instalacja agenta ochrony antymalware możliwa jest na wspieranych systemach Windows, Mac oraz Linux.

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

1. Microsoft Edge
2. Mozilla Firefox
3. Google Chrome
4. Safari

Zarówno konsola, jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów muszą posiadać polski interfejs użytkownika.

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

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

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie musi posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.

3. Rozwiązanie musi obsługiwać technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie musi umożliwiać wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie musi posiadać możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie musi chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie musi posiadać mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie musi posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. System musi zapewniać możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie musi posiadać możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie musi posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie musi posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie musi posiadać możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie musi posiadać możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.

25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie musi posiadać funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta musi w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie musi posiadać możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie musi posiadać możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
37. Rozwiązanie musi posiadać możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie musi posiadać możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
39. Rozwiązanie musi powiadamiać automatycznie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
40. Rozwiązanie musi posiadać możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie musi posiadać możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie musi umożliwiać blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie musi posiadać możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.

45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skrypty ActiveX i pobierane pliki.
46. Rozwiązanie musi posiadać możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie musi umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie musi zapewniać co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie musi umożliwiać blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie musi posiadać wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – system musi zapewniać administratorowi możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie musi posiadać wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Rozwiązanie musi posiadać funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
58. Rozwiązanie musi pozwalać na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
59. Rozwiązanie musi posiadać możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
60. Rozwiązanie musi umożliwiać stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
63. Moduł aktualizacji aplikacji, musi skanować okresowo aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
64. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
65. System musi zapewniać administratorowi możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
66. System musi zapewniać administratorowi możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.

67. Mechanizm aktualizacji aplikacji musi umożliwiać automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, system musi zapewniać administratorowi możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
71. System musi zapewniać administratorowi możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
72. Rozwiązanie musi umożliwiać wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
74. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
75. Mechanizm kontroli urządzeń zewnętrznych musi obsługiwać m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
76. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
78. Rozwiązanie musi posiadać możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
79. Mechanizm kontroli urządzeń musi umożliwiać blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
80. Rozwiązanie musi posiadać opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
82. Rozwiązanie musi posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
83. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
84. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
85. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
86. System musi zapewniać administratorowi możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
87. System musi zapewniać administratorowi możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
88. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na

ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

89. Moduł musi posiadać możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
90. System musi zapewniać administratorowi możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
91. System musi zapewniać możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
92. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
93. Rozwiązanie musi posiadać funkcjonalność kontroli uruchamianych aplikacji.
94. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji
95. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
96. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
97. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
98. System musi umożliwiać administratorowi, podczas konfiguracji procesu szyfrowania, wymuszenie od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
99. Rozwiązanie musi posiadać możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
100. Rozwiązanie musi pozwalać na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
101. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
102. Rozwiązanie musi pozwalać na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
103. System musi zapewniać administratorowi możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
104. Rozwiązanie musi pozwalać na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
105. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.
3. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.

4. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).
5. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
6. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
7. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
8. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
9. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
10. Rozwiązanie musi posiadać dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
11. System musi zapewniać możliwość eksportu listy wszystkich hostów do pliku CSV.
12. System musi zapewniać administratorowi możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
13. System musi zapewniać administratorowi możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
14. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
15. Rozwiązanie musi posiadać dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
16. System musi zapewniać możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
17. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
18. Po wskazaniu danej poprawki system musi zapewniać administratorowi możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
19. System musi zapewniać administratorowi możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
20. Rozwiązanie musi posiadać moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
21. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
22. Rozwiązanie musi posiadać wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
23. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

24. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
25. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
26. Rozwiązanie musi zapewniać możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
27. Profile mogą być przypisane do pojedynczych hostów lub do grup.
28. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
29. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
30. System musi zapewniać możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
31. Rozwiązanie musi umożliwiać administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
32. Z poziomu portalu zarządzającego system musi zapewniać możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
33. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
34. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
35. System musi zapewniać administratorowi możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
36. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows, który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
37. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
38. Konsola musi posiadać możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
39. W ramach posiadanych licencji system musi zapewniać możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
40. Konsola musi posiadać wbudowane narzędzie umożliwiające wygenerowanie podsumowania zdarzeń bezpieczeństwa z okresu ostatnich 7 dni.
41. Narzędzie w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
42. Wygenerowane podsumowanie zdarzeń bezpieczeństwa dostępne jest w języku wykorzystywanym w konsoli
43. Korzystanie z narzędzia nie wymaga posiadania dodatkowej licencji.
44. System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.
45. 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.

46. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania ekspozycją na atak (Exposure Management) – 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.
47. Rozwiązanie musi posiadać polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.
48. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, musi zapewniać możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
49. Agent instalowany na stacjach końcowych i serwerach musi posiadać możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
50. Agent instalowany na stacjach końcowych i serwerach musi posiadać możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
51. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
52. 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.
53. Agent instalowany na stacjach końcowych i serwerach musi monitorować i zbiera informacje na temat co najmniej następujących zdarzeń:
 - a) dostęp do pliku;
 - b) tworzenie nowego procesu;
 - c) nawiązane połączenia sieciowe;
 - d) wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - e) zawartość skryptów uruchamianych na monitorowanej stacji.
54. 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.
55. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączności sieciowych.
56. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
57. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
58. 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.
59. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
60. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
61. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
62. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.

63. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
64. Rozwiązanie musi posiadać możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
65. Każda detekcja zawiera co najmniej następujące informacje:
 - a) Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
 - b) Data i czas wystąpienia podejrzanych zdarzeń.
 - c) Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
 - d) Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
 - e) Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
 - f) Poziom ryzyka, określający istotność danej detekcji.
 - g) Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
66. 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).
67. 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).
68. Rozwiązanie musi umożliwiać oznaczanie wygenerowanych detekcji jako błędne.
69. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
70. Rozwiązanie musi posiadać możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
71. Rozwiązanie musi pozwalać na dodanie własnego komentarza przy wykrytej detekcji.
72. Rozwiązanie musi umożliwiać wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
73. Rozwiązanie musi pozwalać na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
74. Rozwiązanie musi pozwalać na izolację sieciową komputerów przez administratora.
75. Rozwiązanie musi umożliwiać tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
76. Rozwiązanie musi umożliwiać 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.
77. Rozwiązanie musi umożliwiać tworzenie raportów
78. Rozwiązanie musi zapewniać dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
79. Konsola centralnego zarządzania, musi oferować interfejs w języku Polskim.
80. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym System musi zapewniać administratorowi możliwość weryfikacji stanu bezpieczeństwa organizacji.

81. Rozwiązanie musi umożliwiać 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.
82. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
83. 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.
84. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
85. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania ekspozycją na atak (Exposure Management).
86. Dodanie klucza licencyjnego skutkuje aktywowaniem zawartości zakładki obsługującej dany produkt w portalu zarządzającym.
87. Rozwiązanie musi posiadać wbudowane narzędzie pozwalające na stworzenie podsumowania incydentu na podstawie dostępnych danych.
88. Narzędzie umożliwiające stworzenie podsumowania incydentu w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
89. Generowane podsumowanie incydentu dostępne jest w języku wykorzystywanym w konsoli zarządzającej.
90. Rozwiązanie musi pozwalać na wykupienie dodatkowych usług monitorowa oraz monitorowania i reakcji (MDR) na incydenty dla systemu EDR, które realizowane są przez zespoły bezpieczeństwa producenta rozwiązania.
91. Wykupienie usługi nie ogranicza administratorowi dostępu do konsoli zarządzającej i nie wymaga reinstalacji agentów.

Moduł CTEM

1. Rozwiązanie musi zapewniać monitorowanie ekspozycji na potencjalny atak środowiska informatycznego organizacji.
2. Zarządzanie ekspozycją na atak odbywa się na wielu poziomach: detekcji obiektów znajdujących się w sieci lokalnej, skanowaniu w poszukiwaniu podatności, skanowaniu usług web, monitorowaniu tożsamości na poziomie Entra ID,
3. W przypadku posiadania odpowiedniej licencji rozwiązanie umożliwia skanowaniu słabych punktów konfiguracji usług chmurowych wykorzystywanych w usługach Amazon (AWS) oraz MS Azure.
4. Wszystkie mechanizmy związane z zarządzaniem ekspozycją na atak zarządzane i konfigurowane są z jednej konsoli zarządzającej.
5. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.
6. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta
7. Konsola zarządzania musi oferować dostęp za pomocą następujących wspieranych przeglądarek internetowych:
8. Microsoft Edge
9. Mozilla Firefox
10. Google Chrome

11. Safari
12. Konsola zarządzająca dostępna jest w języku polskim.
13. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.
14. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.
15. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).
16. Konsola wyposażona jest w panel kontrolny, w którym wyświetlane są informacje podsumowujące dotyczące poziomu bezpieczeństwa chronionej organizacji.
17. Ta sama konsola umożliwia zarządzanie innymi produktami w przypadku posiadania odpowiedniej licencji w tym co najmniej ochrony antymalware, systemem EDR, ochroną usług Microsoft 365
18. Konsola musi pozwalać na podgląd posiadanych licencji.
19. Rozwiązanie na podstawie uzyskanych wyników pochodzących z monitorowanego środowiska wskazuje administratorowi krytyczne detekcje, które powinny zostać naprawione w 1 kolejności w celu przerwania potencjalnej ścieżki ataku.
20. Poza najbardziej krytycznymi rekomendacjami, rozwiązanie pozwala administratorowi na przegląd wszystkich nieprawidłowości wykrytych przez wykorzystywane mechanizmy skanujące.
21. Rozwiązanie w swoim działaniu wykorzystuje mechanizmy umożliwiające graficzne tworzenie ścieżek potencjalnego ataku.
22. Rozwiązanie musi posiadać wbudowany panel kontrolny, za pomocą którego administrator ma podgląd na aktualny poziom bezpieczeństwa organizacji.
23. Dedykowany panel kontrolny dla mechanizmu zarządzania ekspozycją na atak, zawiera dynamiczne diagramy wskazujące na którym poziomie monitorowania bezpieczeństwa organizacji jest najniższy (poziom sieciowy, urządzeń, tożsamości, usług chmurowych).
24. Rekomendacje wymagające najpilniejszych działań zawierają informacje o: typie rekomendacji, lokalizacji działań naprawczych (na poziomie: usług chmurowych, urządzeń, tożsamości, sieci), wielkość nakładu pracy wymaganego do naprawienia wykrytej nieprawidłowości.
25. Panel kontrolny wskazuje administratorowi obiekty stanowiące największe zagrożenie dla poziomu bezpieczeństwa organizacji.

Mechanizm skanowania w poszukiwaniu podatności:

1. Rozwiązanie musi realizować skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku organizacji, zarządzanego z poziomu konsoli centralnego zarządzania.
2. Oprogramowanie skanujące podatności bez agentowo (lokalny scan node) dostępne jest w postaci aplikacji instalowanej lokalnie na wspieranych systemach Windows oraz linux
3. Rozwiązanie musi umożliwiać również agentowe skanowanie w poszukiwaniu podatności na komputerach z systemem Windows.
4. Ten sam agent zainstalowany na wspieranych systemach Windows w przypadku posiadania odpowiedniej licencji może dodatkowo zapewniać również ochronę antymalware i funkcjonalność systemu EDR.
5. Skanowanie agentowe odbywać się może w cyklach co:4,6,12,24 godzin
6. System musi zapewniać możliwość włączenia i wyłączenia funkcji skanowania agentowego.
7. Wyłączenie funkcji skanowania agentowego nie powoduje deinstalacji agenta na danym hoście.

8. Rozwiązanie musi umożliwiać przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.
9. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:
10. wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.
11. wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.
12. Pozwala na konfigurację parametrów skanowania takich jak:
 - a) zakres przeszukiwanych portów (osobne wartości dla TCP i UDP)
 - b) wydajność skanowania (6 poziomów),
 - c) liczbę jednoczesnych wątków skanowania (1,2,4,8,16,24,32)
 - d) możliwość wykrycia wersji systemu operacyjnego.
13. konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)
14. określenia maksymalnej ilości wykonanych skanowań (1-100) lub bez ograniczenia.
15. konfigurację wysyłania powiadomień na wskazane adresy e-mail
16. powiadomienia dotyczyć mogą: informacji o rozpoczęciu skanowania, jego zakończeniu, zmiany ilości hostów w stosunku do poprzedniego skanowania, zmiany ilości portów w stosunku do poprzedniego skanowania.
17. Konsola zarządzająca musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.
18. Widok listy dostępnych skanowań wykrywających obiekty pozwala na zaawansowane filtrowanie.
19. Konsola musi pozwalać na uruchomienie z poziomu listy dostępnych skanowań, wskazanego skanowania wykrywającego obiekty na żądanie z pominięciem harmonogramu.
20. Trwające zadanie skanowania w poszukiwaniu obiektów może zostać przerwane na żądanie.
21. Konsola zarządzania musi umożliwiać eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLSX oraz XML.
22. Rozwiązanie musi umożliwiać uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.
23. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:
24. określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.
25. masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.
26. konfigurację parametrów skanowania, takich jak:
 - a) zakres skanowanych portów sieciowych TCP/UDP,
 - b) parametr wydajności skanowania (6 poziomów)
 - c) rodzaj uwierzytelniania na skanowanej stacji.
27. konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.
28. konfigurację wysyłania powiadomień na wskazane adresy e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
29. W przypadku tworzonego zadania skanowania system musi zapewniać administratorowi możliwość określenia czy do celu skanowania mają zostać wykorzystane wszystkie dostępne pluginy skanujące, tylko wybrane, wszystkie pluginy poza wskazanymi.

30. System musi zapewniać administratorowi możliwość podglądu dostępnych pluginów skanujących podatności i przeszukiwania ich listy.
31. Konsola zarządzania musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa.
32. Konsola musi pozwalać na uruchomienie i zatrzymanie skanowania w poszukiwaniu znanych podatności na żądanie.
33. Konsola zarządzania musi umożliwiać eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku docx i xml
34. Dla danego hosta widoczne są wyniki skanowania w poszukiwaniu podatności.
35. Wyniki zawierają listę wykrytych podatności wraz z poziomem ich krytyczności
36. Dla danej wykrytej podatności dostępny jest: jej opis, poziom krytyczności w oparciu o punktację CVSS, datę wykrycia, wersję pluginu który wykrył podatność, sugestię rozwiązania (jeśli jest dostępna), informację o publicznie dostępnym exploitie (jeśli jest dostępna), zewnętrzne referencje (jeśli są dostępne).
37. Rozwiązanie musi umożliwiać uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.
38. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:
 - a) określenie skanowanego celu za pomocą adresu URL.
 - b) konfigurację parametrów skanowania takich jak:
 - i) rodzaje testowanych ataków,
 - ii) wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),
 - iii) parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).
 - c) konfigurację uwierzytelniania w testowanej aplikacji web.
 - d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca oraz wskazanie godziny rozpoczęcia skanowania.
 - e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
 - f) Konsola zarządzania musi umożliwiać podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych
 - g) Rozwiązanie musi umożliwiać skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.
 - h) Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:
 - i) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.
 - j) zapisywanie wskazanych warunków wyszukiwania jako szablony.
 - k) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.
 - l) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.
 - m) Rozwiązanie musi umożliwiać podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.
39. Lista wszystkich wykrytych podatności musi umożliwiać:
 - a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (tag), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia,

- b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.
 - c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.
40. Rozwiązanie musi umożliwiać utworzenie nowego raportu podsumowującego wykryte podatności.
41. Rozwiązanie musi umożliwiać podgląd listy wygenerowanych raportów
42. Raport podsumowujący umożliwia:
- a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,
 - b) wybranie grup urządzeń, które będą znajdowały się w raporcie,
 - c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,
 - d) Utworzenie harmonogramu generowania raportu
 - e) Wskazanie adresu email na który zostanie wysłany link udostępniający wygenerowany raport, wraz z określeniem czasu ważności linku
43. Lista wygenerowanych raportów musi umożliwiać:
- a) Wygenerowanie raportu na żądanie
 - b) eksport wyniku raportu do pliku XML(pogrupowany hostami), DOCX(pogrupowany hostami lub wykrytymi podatnościami lub podsumowujący), XLSX (pogrupowany wykrytymi podatnościami)
44. System musi zapewniać administratorowi możliwość określenia: strefy czasowej dla swojej organizacji, długości przetrzymywania raportów (miesiąc, kwartał, pół roku, rok, 2 lata)
45. Dostęp do konsoli może być ograniczony na podstawie adresów IP lub ich zakresu.

MONITOROWANIE TOŻSAMOŚCI NA POZIOMIE EntraID

1. Rozwiązanie musi pozwalać na monitorowanie tożsamości znajdujących się w ramach usługi Entra ID
2. Aktywacja synchronizacji pomiędzy systemem monitorującym a usługą Entra ID odbywa się przy wykorzystaniu dedykowanego kreatora wbudowanego w system.
3. System musi zapewniać administratorowi w ramach konsoli dostęp do dedykowanej zakładki zawierającej listę tożsamości objętych monitorowaniem przez system.
4. Lista tożsamości zawiera następujące informacje: Konto, Nazwę użytkownika, status ryzyka, Typ, poziom ważności, kontekst biznesowy, informacje dotyczące wykrycia konta w wyciekach danych, status konfiguracji MFA, informację dotyczącą daty ostatniej zmiany hasła.
5. Po wybraniu danego konta, system musi zapewniać administratorowi możliwość zmiany poziomu ważności konta, wartości dostępne to: niska, normalna, wysoka ważność.
6. Zmiana poziomu ważności konta ma wpływ na mechanizm tworzący detekcje.
7. System musi zapewniać administratorowi możliwość ręcznego wprowadzenia komentarza dotyczącego kontekstu biznesowego dla danego konta.
8. Wybierając szczegóły dla danego konta, administrator otrzymuje informacje dotyczące podsumowania konta oraz informacji związanych z ewentualnym ryzykiem dla konta.
9. Informacje związane z zarządzaniem ryzykiem dla konta zawierają: Status ryzyka, informacje czy konto pojawiło się w wycieku danych, opis dotyczący informacji związanych z wyciekiem danych, datę wycieku w którym konto się pojawiło, datę detekcji.
10. System musi zapewniać administratorowi wgląd we wszystkie wykryte nieprawidłowości związane z monitorowanymi kontami,

11. Rozwiązanie na podstawie wykrytych nieprawidłowości na poziomie monitorowanych kont, wskazuje administratorowi sugerowane rozwiązanie danego problemu.

Mechanizm monitorowania bezpieczeństwa konfiguracji usług chmurowych

1. Rozwiązanie musi obsługiwać usługi Amazon AWS oraz Microsoft Azure.
2. Rozwiązanie musi posiadać Panel kontrolny (dashboard) przedstawiający podsumowanie stanu ochrony.
3. Rozwiązanie musi pozwalać na prześledzenie trendów związanych ze zmianą poziomu bezpieczeństwa, na przestrzeni czasu, na podstawie wykonywanych skanowań.
4. Trendy dotyczące zmian poziomu bezpieczeństwa można prześledzić na podstawie określonego okresu czasu: ostatniego miesiąca, ostatnich 2 miesięcy, ostatnich 6 miesięcy, ostatnich 12 miesięcy, ostatnich 18 miesięcy
5. Rozwiązanie musi posiadać dedykowaną zakładkę zawierającą informacje dotyczące skanowań oraz wyników skanowań.
6. Widok skonfigurowanych skanowań zawiera informacje dotyczące: Nazwy skanowań, informacje dotyczące ostatniego statusu skanowania, ilości detekcji, nazwy grup skanowań, częstotliwości skanowań, w przypadku skanowań zgodnie z harmonogramem informacji dotyczącej czasu kiedy odbyło się ostatnie skanowanie oraz daty najbliższego skanowania.
7. System musi zapewniać administratorowi możliwość tworzenia nowych zadań skanowania.
8. Tworzenie nowych zadań skanowania odbywa się za pomocą wbudowanego kreatora.
9. Podczas tworzenia zadania skanowania system musi zapewniać administratorowi możliwość podania nazwy zadania, wskazania grupy reguł jakie mają brać udział w skanowaniu, oraz określenia częstotliwości skanowania w tym: ręcznego skanowania, skanowania raz w tygodniu, skanowania raz w miesiącu.
10. W przypadku wyboru skanowania co tydzień, system musi zapewniać administratorowi możliwość wskazania dnia tygodnia w jakim skanowanie ma się odbywać oraz zakresu godzin pomiędzy którymi skanowanie ma zostać uruchomione – w dzień w godzinach pomiędzy 8-20, lub nocą pomiędzy 20-8.
11. System musi zapewniać administratorowi możliwość wskazania posiadanych kont chmurowych dla których zostanie przeprowadzone skanowanie.
12. W przypadku posiadania usług u kilku dostawców usług chmurowych system musi zapewniać możliwość wskazania jednego lub kilku kont, które zostaną objęte skanowaniem.
13. Po utworzeniu zadania skanowania, system musi zapewniać administratorowi możliwość jego natychmiastowego uruchomienia z poziomu menu.
14. Po wybraniu zadania skanowania, administrator uzyskuje wgląd w listę skanowań, które odbyły się na przestrzeni czasu.
15. Lista skanowań zawiera informacje dotyczące daty skanowania, jego stanu, ilości detekcji i ich poziomu krytyczności oraz liczby kont chmurowych objętych skanowaniem.
16. Wynik skanowania zawiera informacje dotyczące wykrytych nieprawidłowości, dostawcę usługi chmurowej dla której zostały wykryte nieprawidłowości, poziom krytyczności detekcji, informację dotyczącą nakładu pracy wymaganego do naprawy wykrytej nieprawidłowości, ilości zasobów na których nieprawidłowość została wykryta podczas skanowania.
17. Wyniki skanowania mogą być filtrowane w oparciu o: nazwę detekcji, dostawcę usługi chmurowej, poziomu krytyczności, nakładu pracy wymaganego do naprawy wykrytej nieprawidłowości.
18. Szczegóły detekcji zawierają: opis wykrytej nieprawidłowości, opis ryzyka jaki za sobą niesie, nakład pracy wymagany do naprawy, informacje dotyczące sposobu usunięcia nieprawidłowej konfiguracji, linki do zewnętrznych opisów związanych z detekcją.
19. Rozwiązanie musi posiadać wbudowane ponad 160 reguł obejmujący wykrywanie nieprawidłowych konfiguracji w AWS i Azure.

20. System musi zapewniać administratorowi możliwość podglądu dostępnych reguł skanowań.
21. Z listy dostępnych reguł skanowań, system musi zapewniać administratorowi możliwość zaznaczenia wielu reguł i dodania ich do grupy reguł skanowania, które mogą być wykorzystane podczas tworzenia zadań skanowań.

Oprogramowanie do centralnego zarządzania infrastrukturą IT i stacjami roboczymi

Wymagania ogólne dla systemu zarządzania

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agent/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
6. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
7. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną pracę wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
8. Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
9. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
10. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
11. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
12. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
13. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
14. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
15. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.
16. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
17. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.

18. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
19. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
20. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
21. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
22. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
23. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
24. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
25. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
26. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
27. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
28. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
29. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
30. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
31. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
32. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
2. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
3. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.

4. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
5. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
6. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
7. Oprogramowanie musi umożliwiać analizę sprzętową:
8. płyty głównej w zakresie model, producent, nr. seryjny,
9. CPU w zakresie nazwy, modelu, producenta, częstotliwości,
10. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
11. RAM w zakresie wielkości pamięci,
12. karty sieciowej w zakresie model, adres IP, adres MAC,
13. karty graficznej w zakresie model.
14. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
15. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
16. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
17. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
18. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
19. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
20. Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
21. Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
22. Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
23. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
2. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
3. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
4. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
5. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
6. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.

7. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
8. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
9. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
10. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
2. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
3. w procesie automatycznego audytu licencji (rozliczenie ilościowe).
4. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
5. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
6. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

CMDB

1. Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
2. Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
3. Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
4. Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
5. Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
6. Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
7. Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej
8. Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
9. Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami
10. Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
11. Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
12. Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
13. Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
14. Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
15. Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami

1. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
2. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
3. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
4. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
5. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
6. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
7. Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
8. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
9. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
10. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
11. Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
12. Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
13. Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
14. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
15. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
16. Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
17. Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
18. Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
19. Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
20. Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
21. Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
22. Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
23. Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
24. Oprogramowanie musi udostępniać kreator raportów dla zasobów
25. Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
26. Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
27. Oprogramowanie musi umożliwiać ewidencję magazynów
28. Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
29. Oprogramowanie musi umożliwiać ewidencję produktów magazynowych

30. Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
31. Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
32. Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
33. Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
34. Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
35. Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
36. Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
37. Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
38. Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
39. Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
40. Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
41. Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
42. Oprogramowanie musi umożliwiać zarządzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
43. Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

Zdalny pulpit, zdalne zarządzanie komputerem

1. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
2. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
3. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
5. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
6. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
7. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
8. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
9. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
10. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
11. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
12. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
13. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
14. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
15. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN

16. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połączenie konsoli ze wskazanym serwerem aplikacji.
17. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

1. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
2. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
3. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
4. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
5. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
6. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
7. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
8. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
9. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
10. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
11. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
12. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
13. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
14. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
15. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
16. Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi

17. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
18. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
19. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
20. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
21. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
22. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
23. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
24. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
25. Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
26. Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
27. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
2. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
3. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
4. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
5. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
6. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
7. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage

1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
2. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
3. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
4. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage

5. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring stanowisk komputerowych

1. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
2. Oprogramowanie musi umożliwiać zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
3. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
4. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
5. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
6. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
7. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
8. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
9. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
10. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
11. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
12. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
13. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
14. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
15. Oprogramowanie po zainstalowaniu musi przysyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z którego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
16. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

ServiceDesk – Zarządzanie zgłoszeniami

1. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:
 - a) Zarządzanie problemem
 - b) Zarządzanie incydem
 - c) Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
 - d) Zarządzanie umowami serwisowymi
 - e) Definicje poziomów SLA (reakcja, naprawa, reklamacja)
2. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.

3. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
4. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
5. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
6. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
7. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
8. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
9. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
10. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
11. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
12. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
13. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
14. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
15. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. System musi także zapewniać użytkownikowi możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
16. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
17. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
18. Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
19. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
20. Oprogramowanie musi umożliwiać przysyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
21. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
22. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
23. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
24. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
25. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
26. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
27. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
28. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
29. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).

30. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
31. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
32. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
33. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
34. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
35. Oprogramowanie musi umożliwiać przysyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
36. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
37. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
38. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
39. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
40. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
41. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
42. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:
 43. Zmiana statusu po przejściu zgłoszenia przez opiekuna.
 44. Przejmowanie zadań po przejściu zgłoszenia przez opiekuna.
 45. Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
 46. Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
 47. Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
 48. Zamykanie zgłoszenia po upływie czasu reklamacji.
 49. Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
 50. Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
 51. Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
 52. Systemowe potwierdzanie realizacji zgłoszenia.
 53. Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
54. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
55. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
56. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
57. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

58. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
59. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
60. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
61. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
62. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
63. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
64. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
65. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
66. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
67. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
68. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
69. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
70. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
71. Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
72. Oprogramowanie musi umożliwiać definiowanie obiegu za pomocą graficznego/blokowego kreatora.
73. Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
74. Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
75. Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
76. Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
77. Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
78. Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
79. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
80. Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
81. Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
82. Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
83. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

ServiceDesk – Zarządzanie wnioskami

1. Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).

2. Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
3. Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

1. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
2. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
3. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
4. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
5. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
6. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
7. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
8. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
9. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
10. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
11. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
12. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – Zarządzanie rezerwacjami

1. Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
2. Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
3. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
4. Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
5. Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
6. Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Monitoring sieci LAN

1. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony

2. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować o błędach takich jak brak papieru, zacięcie papieru.
3. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
4. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
5. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
6. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
7. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
8. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Zarządzanie dokumentami

1. Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
2. Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
3. Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
4. Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
5. Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
6. Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
7. Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
8. Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

Wymagania formalne:

1. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
2. Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym supportem producenta, liczonym od daty zakończenia wdrożenia.
3. Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
4. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 50 stanowisk komputerowych z systemem klasy Microsoft Windows oraz 40 urządzeń mobilnych z systemem android. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencję dostępową do konsoli zarządzającej
5. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.
6. Zamawiający wymaga od wykonawcy, aby w terminie 20 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagane co najmniej 2 sesje – 4 godzinne)
7. Zamawiający wymaga, aby producent oferowanego oprogramowania przedstawił potwierdzenie (certyfikat), że oprogramowanie wytwarzane jest zgodnie z normą ISO27001.
8. Wymagania dotyczące zgodności z najlepszymi praktykami ITSM:
9. Zamawiający wymaga, aby oferowane oprogramowanie w zakresie:

- a) Zarządzanie incydentami (Incident Management),
- b) Zarządzanie problemami (Problem Management),
- c) Zarządzanie bazą wiedzy (Knowledge Management),
- d) Zarządzanie zasobami (Asset Management).

posiadało aktualny certyfikat zgodności z najlepszymi praktykami IT Service Management, wydany przez niezależną organizację certyfikującą (np. Pink Elephant)

10. Do oferty należy dołączyć kopię stosownego certyfikatu oraz wskazać link do strony internetowej organizacji certyfikującej, na której potwierdzona jest zgodność oferowanego rozwiązania z ww. procesami ITSM.

III. Rozwiązanie klasy UTM do segmentacji sieci i VPN do serwerowni i SUW

Typ I – SUWy 3 sztuki

Wymagania Ogólne

1. 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.
2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. System musi umożliwiać dedykowanie co najmniej 5 administratorów do poszczególnych instancji systemu.
4. System musi obsługiwać protokoły IPv4 oraz IPv6 w zakresie:
 - a) Firewall.
 - b) Ochrony w warstwie aplikacji.
 - c) Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
2. 4 portami Gigabit Ethernet RJ-45.
3. System Firewall musi posiadać wbudowany port konsoli szeregowej.
4. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
3. Translację jeden do jeden oraz jeden do wielu.
4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
5. W ramach systemu system musi zapewniać możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
7. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
9. 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.
10. Amazon Web Services (AWS).
11. Microsoft Azure.
12. Cisco ACI.
13. Google Cloud Platform (GCP).
14. OpenStack.
15. VMware NSX.
16. Kubernetes.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19, 20.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
9. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
10. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
11. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
12. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
13. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
14. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie zapewnia obsługę:
2. Routingu statycznego.
3. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
4. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
5. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
6. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.

7. BFD (Bidirectional Forwarding Detection).
8. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych system musi zapewniać możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System musi współpracować 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. System musi zapewniać administratorowi systemu możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
7. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
5. System musi zapewniać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
6. System musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

Serwisy i licencje

1. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:
2. 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 [x] miesięcy.

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres [x] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Rozszerzone wsparcie serwisowe AHB/SOS

1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania muszą być potwierdzone dokumentami:***** Wymagany jest serwis AHB 24x7x8 *****
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania muszą być potwierdzone dokumentami:

Opisy do wymagań ogólnych

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

Typ II – Serwerownia - 1 sztuka

Wymagania Ogólne

1. 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.

2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
4. System musi umożliwiać dedykowanie co najmniej 5 administratorów do poszczególnych instancji systemu.
5. System musi obsługiwać protokoły IPv4 oraz IPv6 w zakresie:
6. Firewall.
7. Ochrony w warstwie aplikacji.
8. Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
2. 5 portami Gigabit Ethernet RJ-45.
3. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
4. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) - minimum 2 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
3. Translację jeden do jeden oraz jeden do wielu.
4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
5. W ramach systemu system musi zapewniać możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
7. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
9. 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.
10. Amazon Web Services (AWS).
11. Microsoft Azure.
12. Cisco ACI.
13. Google Cloud Platform (GCP).
14. OpenStack.
15. VMware NSX.
16. Kubernetes.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19, 20.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
9. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
10. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
11. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
12. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
13. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
14. 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

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych system musi zapewniać możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System musi współpracować 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

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

Kontrola aplikacji

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

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

3. System musi zapewniać możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System musi zapewniać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

Serwisy i licencje

1. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:
2. 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 [x] miesięcy.

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres [x] 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. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.

2. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.
3. Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz certyfikat potwierdzający posiadany najwyższy poziom certyfikacji technicznej producenta .

Rozszerzone wsparcie serwisowe AHB/SOS

1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania muszą być potwierdzone dokumentami:
2. Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
3. Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

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

IV. Wysokowydajny system deduplikacji danych na potrzeby kopii zapasowych zintegrowany z dedykowanym oprogramowaniem do backupu.

1. System musi umożliwiać wykonywanie kopii zapasowych co najmniej 5 maszyn wirtualnych pracujących w środowisku klastrowym.
2. System musi umożliwiać wykonywanie kopii zapasowych maszyn wirtualnych bez konieczności instalowania agentów wewnątrz każdej chronionej maszyny.
3. System musi umożliwiać wykonywanie kopii pełnych, przyrostowych oraz syntetycznych kopii pełnych.

4. System musi umożliwiać wykonywanie kopii zapasowych danych o łącznej wielkości co najmniej 1 TB oraz zapewniać przestrzeń umożliwiającą wielowersyjne przechowywanie kopii zgodnie z przyjętą polityką retencji.
5. Urządzenie przeznaczone do składowania kopii zapasowych musi posiadać co najmniej 8 TB użytkowej przestrzeni dyskowej dostępnej dla danych backupowych.
6. Urządzenie musi umożliwiać zwiększenie pojemności przestrzeni przeznaczonej na kopie zapasowe bez konieczności wymiany całego urządzenia.
7. System musi realizować sprzętowo lub programowo-sprzętowo deduplikację danych przeznaczonych do zapisu w repozytorium kopii zapasowych.
8. Deduplikacja musi działać automatycznie podczas zapisu danych i nie może wymagać wykonywania ręcznych operacji przez administratora.
9. System musi umożliwiać kompresję danych kopii zapasowych w celu ograniczenia zajmowanej przestrzeni dyskowej.
10. System musi umożliwiać kontrolę integralności przechowywanych danych oraz wykrywanie uszkodzeń danych kopii zapasowych.
11. System musi umożliwiać zabezpieczenie wybranych kopii zapasowych przed modyfikacją lub usunięciem przez określony przez administratora czas.
12. Administrator systemu musi posiadać możliwość definiowania okresu retencji dla poszczególnych zadań wykonywania kopii zapasowych.
13. System musi umożliwiać odtworzenie całej maszyny wirtualnej z wykonanej kopii zapasowej.
14. System musi umożliwiać odtworzenie pojedynczych dysków wirtualnych maszyny.
15. System musi umożliwiać odtworzenie pojedynczych plików i katalogów bez konieczności odtwarzania całej maszyny wirtualnej.
16. System musi umożliwiać szybkie uruchomienie maszyny wirtualnej bezpośrednio z kopii zapasowej lub zastosowanie rozwiązania równoważnego pozwalającego ograniczyć czas niedostępności systemu.
17. System musi umożliwiać wykonywanie kopii zapasowych aplikacji pracujących wewnątrz maszyn wirtualnych z zachowaniem spójności danych.
18. System musi umożliwiać automatyczną weryfikację poprawności wykonania zadań backupowych.
19. System musi umożliwiać przeprowadzenie testowego odtworzenia maszyny wirtualnej w sposób niezakłócający pracy środowiska produkcyjnego.
20. System musi umożliwiać centralne zarządzanie zadaniami backupu, retencją, repozytoriami oraz procesami odtwarzania.
21. System musi umożliwiać tworzenie harmonogramów wykonywania kopii zapasowych z możliwością określenia dni, godzin oraz częstotliwości wykonywania zadań.
22. System musi umożliwiać wysyłanie powiadomień o poprawnym lub błędnym wykonaniu zadań backupowych co najmniej za pomocą poczty elektronicznej.
23. System musi umożliwiać generowanie raportów z wykonania kopii zapasowych oraz operacji odtwarzania.
24. System musi umożliwiać definiowanie kont administracyjnych oraz nadawanie im różnych poziomów uprawnień.
25. System musi umożliwiać szyfrowanie danych kopii zapasowych podczas transmisji oraz przechowywania.
26. Urządzenie backupowe musi posiadać co najmniej dwa redundantne zasilacze umożliwiające pracę urządzenia w przypadku awarii jednego z nich.
27. Urządzenie backupowe musi posiadać interfejsy sieciowe umożliwiające komunikację z prędkością co najmniej 10 Gb/s.

28. Urządzenie musi umożliwiać współpracę z oprogramowaniem backupowym z wykorzystaniem zoptymalizowanego mechanizmu przesyłania danych ograniczającego obciążenie sieci i ilość przesyłanych danych.
29. System musi umożliwiać wykonywanie dodatkowej kopii danych do innego repozytorium lub lokalizacji.
30. System musi umożliwiać replikację lub kopiowanie wybranych kopii zapasowych do drugiego repozytorium w celu zwiększenia odporności na awarie i incydenty bezpieczeństwa.
31. System musi posiadać licencje umożliwiające ochronę minimum 5 maszyn wirtualnych.
32. Licencjonowanie systemu nie może powodować konieczności zakupu dodatkowych licencji wyłącznie z powodu zwiększenia liczby fizycznych procesorów lub rdzeni w hostach klastra, jeżeli liczba chronionych maszyn wirtualnych nie ulega zwiększeniu.
33. Wykonawca musi dostarczyć komplet wymaganych licencji, subskrypcji oraz praw do aktualizacji niezbędnych do prawidłowego działania całego rozwiązania przez okres minimum 36 miesięcy.
34. Wykonawca musi zapewnić minimum 36 miesięcy wsparcia technicznego dla dostarczonego urządzenia i oprogramowania.
35. W ramach zamówienia Wykonawca musi wykonać instalację, konfigurację oraz integrację systemu z istniejącym środowiskiem wirtualizacyjnym Zamawiającego.
36. W ramach wdrożenia Wykonawca musi skonfigurować zadania wykonywania kopii zapasowych dla wskazanych przez Zamawiającego maszyn wirtualnych.
37. Wykonawca musi skonfigurować politykę retencji, deduplikację, kompresję oraz mechanizmy zabezpieczające kopie przed nieuprawnionym usunięciem lub modyfikacją.
38. Wykonawca musi przeprowadzić test wykonania kopii zapasowej oraz test odtworzenia co najmniej jednej kompletnej maszyny wirtualnej i jednego wskazanego pliku.
39. Wykonawca musi przekazać Zamawiającemu dokumentację powdrożeniową zawierającą co najmniej opis konfiguracji, harmonogramy kopii, polityki retencji, sposób odtwarzania danych oraz podstawowe procedury administracyjne.
40. Wykonawca musi przeprowadzić instruktaż administratorów Zamawiającego w zakresie obsługi, monitorowania, wykonywania kopii oraz odtwarzania danych.

V. Serwer z oprogramowaniem - 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1. serwerowa do montażu w szafie RACK 19" o wysokości maksymalnie 2U 2. Obudowa z możliwością wyposażenia w kartę do bezpośredniej komunikacji z urządzeniem mobilnym. 3. Obudowa musi posiadać zainstalowany panel LCD umieszczony na froncie obudowy i pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze). 4. serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

Parametr	Charakterystyka (wymagania minimalne)
	5. W obudowie musi być zainstalowany zestaw redundantnych wentylatorów.
Zasilanie	6. W obudowie musi być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 1100W w standardzie Titanium każdy wymienialnych podczas pracy oraz 2 kable C13/C14 10A minimum 2m
Płyta główna	7. Płyta główna z możliwością zainstalowania dwóch procesorów. 8. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 9. musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust), 10. Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. 11. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 V3
Chipset	12. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	13. Dwa procesory typu skalowalnego z uwagi na licencjonowanie posiadający dokładnie 8 rdzeni działającego co najmniej z częstotliwością minimum 2.6 GHz i dającego w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ 14. wynik nie mniejszy niż 40 480 pkt. dla wersji Dual CPU na dzień 06.10.2026 r.
RAM	15. Na płycie głównej musi znajdować się minimum 32 sloty przeznaczone do instalacji pamięci taktowaną przynajmniej z częstotliwością 6400MT/s przy użyciu odpowiednich procesorów. 16. 256GB pamięci RAM w modułach 128GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 6400MT/s
Dyski twarde	17. Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski. 18. Miejsce na co najmniej 12 dysków 3.5" wymienialne bez wyłączania systemu. 19. Zainstalowane co najmniej 2 dyski minimum 960GB SSD SATA Read Intensive 6Gbps
Kontroler RAID	20. Serwer musi posiadać kontroler RAID umożliwiający konfigurację RAID 0, 1, 10, 5, 50, 6, 60.
Interfejsy sieciowe/FC/SAS	21. min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BASE-T,

Parametr	Charakterystyka (wymagania minimalne)
	22. min. 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (powyższe porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Video	23. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Elementy montażowe	24. Komplet wysuwanych szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych
Moduł połączeniowy do zarządzania serwerem	25. Technologia serwera musi pozwalać na dodanie modułu umożliwiającego bezprzewodowe zarządzanie serwerem, bez potrzeby fizycznego podłączania się do konsoli ani korzystania z tzw. kart typu crash. 26. Oferowane urządzenie musi: 27. Umożliwiać komunikację z serwerem za pośrednictwem łączności bezprzewodowej (Bluetooth lub Wi-Fi) przy użyciu dedykowanej aplikacji instalowanej na urządzeniach mobilnych (smartfon, tablet) z systemem Android i/lub iOS. 28. Zapewniać administratorowi możliwość: 29. monitorowania stanu serwera, przeglądania logów oraz prowadzenia inwentaryzacji komponentów, 30. konfiguracji serwera, wysyłania poleceń administracyjnych oraz uzyskiwania dostępu do raportów serwisowych, 31. przeprowadzania aktualizacji oprogramowania układowego, uruchamiania narzędzi diagnostycznych i pełnego zarządzania serwerem bez konieczności użycia klawiatury, monitora i myszy. 32. Funkcjonować bez użycia dodatkowych kabli czy kart zewnętrznych, co pozwala na przyspieszenie i uproszczenie pracy administratora w środowiskach serwerowych o dużej gęstości sprzętu (szafy rackowe). 33. Być aktywowane bezpośrednio z poziomu obudowy serwera i umożliwiać łatwe parowanie z urządzeniem mobilnym, np. poprzez kod QR lub standard BLE (Bluetooth Low Energy). 34. Rozwiązanie to musi wspierać administratorów podczas inwentaryzacji, rekonfiguracji infrastruktury serwerowej oraz umożliwiać szybkie reagowanie na komunikaty i alerty systemowe.
Bezpieczeństwo	35. Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 36. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. 37. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

Parametr	Charakterystyka (wymagania minimalne)
	38. BIOS musi umożliwiać przejście do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 39. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 40. Moduł TPM 2.0 41. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 42. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 43. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Kontroler eksploatacji serwera	44. Serwer musi być standardowo wyposażony w kontroler eksploatacji 45. Konfigurowanie ustawień BIOS i sprzętu. 46. Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7. 47. Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. 48. Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. 49. Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. 50. Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. 51. Udostępnianie logów sprzętowych w celu rozwiązywania problemów. 52. Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man 53. Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. 54. Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. 55. Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów. 56. Powrót do poprzedniej wersji oprogramowania układowego. 57. Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode"

Parametr	Charakterystyka (wymagania minimalne)
	58. Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. 59. Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. 60. Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD
Karta Zarządzania	61. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: a) Uwierzytelnianie dwuskładnikowe RSA SecurID (2FA). b) Dostęp do zdalnej konsoli HTML5. c) Obsługa wirtualnych nośników danych. d) Zdalne udostępnianie plików (RFS). e) Współpraca wirtualnej konsoli (do sześciu użytkowników). f) Czat w ramach wirtualnej konsoli g) Zarządzanie kluczami h) Zarządzanie z poziomu portu USB Dual-Mode Type-C znajdującego się na panelu przednim serwera. i) Wirtualny schowek. j) Możliwość uwierzytelniania z wykorzystaniem Simple 2-Factor Authentication (Simple 2FA) k) Zarządzanie kluczami: Secure Enterprise Key Management (SEKM) i Local Key Management (iLKM). l) Automatyczna rejestracja certyfikatów SSL. m) Zaawansowane zarządzanie termiczne. n) Graficzne wyświetlanie zużycia energii w czasie rzeczywistym. o) Historyczne dane zużycia energii. p) Limitowanie zużycia energii (Power Capping). q) Dostosowanie przepływu powietrza PCIe (LFM). r) Zdalne wdrażanie systemu operacyjnego. s) Zapisywanie wideo z awarii systemu. t) Zarządzanie jednostkami przetwarzania danych (DPU). u) Konfiguracja progów zużycia dysków SSD. v) Dynamiczna konfiguracja wirtualnych adresów pamięci masowej.
System operacyjny	62. Zakres Przedmiotu Zamówienia obejmuje dostarczenie 2 sztuk Oprogramowania Systemowego zwanego dalej SSO. Licencje muszą uprawniać do uruchamiania SSO w środowisku fizycznym dowolnej liczby wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Licencja musi pokrywać wszystkie rdzenie procesora. 63. Dodatkowo należy dostarczyć 6 sztuk licencji dostępowych na użytkownika.

Parametr	Charakterystyka (wymagania minimalne)
	a) SSO musi posiadać następujące, wbudowane cechy: możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, d) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, f) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), g) wbudowane wsparcie instalacji i pracy na wolumenach, które: ▪ pozwalają na zmianę rozmiaru w czasie pracy systemu, h) ▪ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, i) ▪ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, j) ▪ umożliwiają zdefiniowanie list kontroli dostępu (ACL), - a) - b) k) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, wbudowane szyfrowanie dysków możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
Oprogramowanie zarządzania	do 64. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: a) wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; b) możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; c) wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH; d) możliwość oskryptowywania procesu wykrywania urządzeń;

Parametr	Charakterystyka (wymagania minimalne)
	e) możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; f) szczegółowy opis wykrytych systemów oraz ich komponentów; g) możliwość eksportu raportu do CSV, HTML, XLS; h) grupowanie urządzeń w oparciu o kryteria użytkownika; i) automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; j) szybki podgląd stanu środowiska; k) podsumowanie stanu dla każdego urządzenia; l) szczegółowy status urządzenia/elementu/komponentu; m) generowanie alertów przy zmianie stanu urządzenia; n) filtry raportów umożliwiające podgląd najważniejszych zdarzeń; o) integracja z service desk producenta dostarczonej platformy sprzętowej; p) możliwość przejęcia zdalnego pulpitu; q) możliwość podmontowania wirtualnego napędu; r) kreator umożliwiający dostosowanie akcji dla wybranych alertów; s) możliwość importu plików MIB; t) przesyłanie alertów „as-is” do innych konsol firm trzecich; u) aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); v) możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; w) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 65. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
Aplikacja do zarządzania	66. Aplikacja mobilna do zarządzania serwerami powinna umożliwiać: a) Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji. b) Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych. c) Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej. d) Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania. e) Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi. f) Konfigurowanie serwerów zdalnie.

Parametr	Charakterystyka (wymagania minimalne)
	g) Wysyłanie poleceń sterowania zasilaniem i innych poleceń. h) Otrzymywanie powiadomień o alertach z systemów zarządzania. i) Pobieranie informacji o gwarancji. j) Uruchamianie zewnętrznych aplikacji, takich jak klienty zdalnego pulpitu. k) Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia. l) Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii. m) Automatyczne wylogowanie w przypadku braku aktywności. n) Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi. o) Wyświetlanie szczegółowych informacji o serwerze oraz dzienników. p) Otrzymywanie automatycznych powiadomień z konsoli zarządzania. q) Przypisywanie adresów IP i modyfikowanie haseł. r) Konfigurowanie atrybutów BIOS. s) Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej. t) Pobieranie danych z systemów zarządzania typu "jeden do wielu". u) Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu. 67. Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami 68. Kryterium stanowi dodatkową punktację.
Opcjonalny moduł do podłączenia aplikacji mobilnej	69. Moduł powinien umożliwiać następujące funkcjonalności: 70. Bezprzewodową komunikację z urządzeniami mobilnymi wykorzystując technologie Bluetooth Low Energy (BLE) lub Wi-Fi. 71. Zapewnienie fizycznego bezpieczeństwa poprzez wymóg fizycznej obecności administratora przy serwerze i naciśnięcia przycisku aktywacyjnego na serwerze lub wirtualnego przycisku na wyświetlaczu LCD w przypadku obudów. Bez aktywacji nie jest możliwa wymiana danych. 72. Ograniczenie zasięgu komunikacji BLE przed uwierzytelnieniem do około 1 metra, a po uwierzytelnieniu do około 5 metrów. Zasięg Wi-Fi wynosi około 5 metrów. 73. Ograniczenie liczby jednoczesnych połączeń BLE do jednego urządzenia mobilnego na serwer. 74. Blokowanie dostępu po wielokrotnych próbach połączenia z użyciem nieprawidłowych danych uwierzytelniających, co skutkuje koniecznością ręcznej reaktywacji modułu. 75. Zabezpieczenie komunikacji BLE z wykorzystaniem protokołu TLS 1.2, wymiany kluczy Diffie-Hellmana (2048-bitowe lub większe liczby pierwsze) oraz szyfrowania AES (128-bitowe klucze symetryczne).

Parametr	Charakterystyka (wymagania minimalne)
	76. Wykorzystanie trybu szyfrowania GCM z unikalnymi numerami sekwencyjnymi w celu ochrony przed nieautoryzowaną ingerencją, ujawnieniem informacji oraz atakami typu replay. 77. Aktywację Wi-Fi tylko w przypadku komunikacji wymagającej większej przepustowości lub komunikacji opartej na IP. 78. Generowanie nowego, losowego klucza WPA2PSK za każdym razem, gdy aktywowane jest Wi-Fi, który jest przesyłany do aplikacji mobilnej za pośrednictwem połączenia BLE. 79. Uwierzytelnianie użytkowników za pomocą tych samych danych uwierzytelniających co do kontrolera zdalnego dostępu. 80. Identyfikację serwera za pomocą certyfikatu PKI w formacie x509 oraz wyświetlanie znacznika serwisowego podczas łączenia. 81. Możliwość aktywacji diody ID LED w celu potwierdzenia połączenia z właściwym systemem. 82. Umożliwienie administratorom zdalnego wyłączenia i włączania serwerów za pomocą poleceń.
Certyfikaty	83. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 84. Serwer musi posiadać deklarację CE. 85. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki muszą być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów musi odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe muszą zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver na terenie Polski według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. a) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja użytkownika	86. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. a) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Parametr	Charakterystyka (wymagania minimalne)
Warunki gwarancji	87. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. 88. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. 89. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 90. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 91. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) musi rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. 92. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 93. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. 94. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 95. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: a) Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. b) Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. c) Reakcja na miejscu u Zamawiającego musi nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. d) Pracownik serwisu musi skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. e) Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową

Parametr	Charakterystyka (wymagania minimalne)
	część i przekazać dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. 96. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 97. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Portal wsparcia produktu	98. W ramach wsparcia technicznego wymagana jest usługa polegająca na przygotowaniu i dostarczeniu spersonalizowanego panelu w chmurze 99. Usługa musi pozwalać na identyfikowanie priorytetów i potencjalnych zagrożeń technicznych sprzętu 100. co pomoże w podejmowanie właściwych działań. 101. Usługa musi spełniać następujące założenia/funkcje: a) Proaktywne zarządzanie priorytetami usług serwisowych w tym graficzną reprezentację poziomu zagrożeń. b) Możliwość personalizacji widoku przez członków zespołu do zarządzanych przez nich lokalizacji i zasobów. c) Dostęp do szczegółów dotyczących sprzętu i oprogramowania, w tym incydentów krytycznych, wsparcia technicznego, eskalacji, konserwacji na miejscu, poziomów kodu, poradników bezpieczeństwa i technicznych, zakresu wsparcia, wymiany części, łączności urządzeń i bram. d) Dostęp do danych historycznych i analiz na potrzeby planowania IT
Aplikacja do zarządzania wsparciem	102. Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. 103. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. 104. Oprogramowanie musi być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. 105. Konfiguracja i zaoferowany poziom wsparcia musi po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia musi się kontaktować z klientem w celu rozwiązania problemu. 106. Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi

Parametr	Charakterystyka (wymagania minimalne)
	umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury. 107. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: a) Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. b) Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. c) Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. 108. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, 109. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: 110. poprawkach i usprawnieniach dotyczących aktualizacji a) dacie wydania ostatniej aktualizacji 111. priorytecie aktualizacji a) zgodność z systemami operacyjnymi b) jakiego komponentu sprzętu dotyczy aktualizacja c) wszystkie poprzednie aktualizacje z informacjami jak powyżej d) wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne 112. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga. 113. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) 114. sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) 115. dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml 116. raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

VI. UPS do SUW i serwerowni

Typ I – Serwerownia 1szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ i topologia	1. Zasilacz awaryjny UPS typu ON-LINE (VFI) z technologią podwójnej konwersji (True Double Conversion), z zerowym czasem przełączania na tryb bateryjny. 2. Konfiguracja 3 fazy na wejściu / 1 faza na wyjściu (3/1). 3. Zasilacz przystosowany do pracy z agregatem prądotwórczym.
Moc	4. Moc pozorna min. 20 kVA, moc czynna min. 18 kW (współczynnik mocy wyjściowej PF = 0,9).
Parametry wejścia	5. Wejście trójfazowe, napięcie 3×400 V, szeroki zakres napięć wejściowych (min. 190–478 VAC przy obciążeniu 0–50% oraz 305–478 VAC przy obciążeniu 50–100%). Częstotliwość 50/60 Hz, zakres pracy 40–70 Hz. Zniekształcenia prądu wejściowego THDi < 5% (3 fazy). Przyłącze wejściowe: zaciski śrubowe (TERMINAL).
Parametry wyjścia	6. Wejście trójfazowe, napięcie 3×400 V, szeroki zakres napięć wejściowych (min. 190–478 VAC przy obciążeniu 0–50% oraz 305–478 VAC przy obciążeniu 50–100%). Częstotliwość 50/60 Hz, zakres pracy 40–70 Hz. Zniekształcenia prądu wejściowego THDi < 5% (3 fazy). Przyłącze wejściowe: zaciski śrubowe (TERMINAL).
Akumulatory i czas podtrzymania	7. Akumulatory szczelne VRLA/AGM, wbudowany zestaw bateryjny (np. w wariantcie BI: 32×12 V / 9 Ah lub odpowiednik systemowy zapewniający wymagane parametry). Czas podtrzymania min. 10 minut przy 50% obciążenia oraz min. 3,5–5 minut przy 100% obciążenia. Wbudowana ładowarka o odpowiednim prądzie do szybkiego ładowania, czas ładowania do 90% pojemności ok. 3 godz. Możliwość rozbudowy o zewnętrzne zestawy bateryjne (Battery Pack / EBM) z automatycznym wykrywaniem; złącze zewnętrznego modułu bateryjnego. Zarządzanie ładowaniem baterii wydłużające ich żywotność oraz funkcja zimnego startu z baterii.
Obejście (bypass) i zabezpieczenia	8. Wbudowany bypass serwisowy (elektroniczny, automatyczny); możliwość zastosowania zewnętrznego bypassu serwisowego (opcja). Złącze awaryjnego wyłączenia zasilania EPO (Emergency Power Off) / REPO. Zabezpieczenia przed przeciążeniem, zwarcim, przegrzaniem, nadmiernym rozładowaniem baterii oraz przepięciami. Automatyczny restart po powrocie zasilania sieciowego.
Komunikacja i zarządzanie	9. Wbudowany czytelny wyświetlacz LCD / panel dotykowy z informacjami o obciążeniu, stanie baterii, napięciach wejścia/wyjścia, dzienniku zdarzeń i ustawieniach. Porty: RS-232, USB-HID, slot na kartę SNMP / zarządzania

Parametr	Charakterystyka (wymagania minimalne)
	sieciowego (opcja), inteligentny slot rozszerzeń. Oprogramowanie producenta do monitoringu i zdalnego zamykania systemów (np. WinPower).Port równoległy umożliwiający łączenie jednostek w celu pracy równoległej (redundancja/zwiększenie mocy).
Obudowa i warunki pracy	10. Obudowa typu TOWER (wolnostojąca), o wymiarach dostosowanych do wbudowanego zestawu bateryjnego (np. ok. 350 × 650 × 890 mm), masa z bateriami ok. 188 kg.Poziom hałasu < 55–60 dB (z odległości 1 m), temperatura pracy 0–40°C, wilgotność względna 0–95% (bez kondensacji).
Certyfikaty i gwarancja	11. Certyfikat CE. 12. Gwarancja producenta min. 24 miesiące

Typ II – SUWy 3szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ i topologia	1. Zasilacz awaryjny UPS typu Line-Interactive z automatyczną regulacją napięcia (AVR – Boost/Buck). Konfiguracja 1 faza na wejściu / 1 faza na wyjściu (1/1). Zastosowana technologia oszczędzania energii.
Moc	2. Moc pozorna min. 1600 VA, moc czynna (skuteczna) min. 960 W.
Parametry wejścia	3. Wejście jednofazowe, napięcie nominalne 230 V, szeroki zakres napięć wejściowych (min. 167–295 VAC). Częstotliwość 50/60 Hz z automatycznym wykrywaniem. Przyłącze wejściowe: zintegrowany przewód z wtyczką sieciową.
Parametry wyjścia	4. Wyjście jednofazowe, napięcie nominalne 230 V (tolerancja ±10%), przebieg napięcia: sinusoida symulowana (przybliżona) w trybie pracy bateryjnej. Typowy czas przełączania na baterię: maks. 4 ms. Przyłącze wyjściowe: min. 5 gniazd typu francuskiego (FR / CEE 7/5) podtrzymanych i zabezpieczonych.
Akumulatory i czas podtrzymania	5. Akumulatory szczelne kwasowo-ołowiowe (VRLA/AGM), bezobsługowe, wymienne przez wykwalifikowany personel. Czas podtrzymania min. 11 minut przy 50% obciążenia oraz min. 2 minuty przy 100% obciążenia. Średni czas ładowania do 8 godzin. Funkcja zimnego startu (uruchomienie z baterii bez zasilania sieciowego).
Zabezpieczenia	6. Zabezpieczenia przed przeciążeniem, zwarcim, nadmiernym rozładowaniem oraz przeładowaniem baterii.Tłumienie przepięć (znamionowa wartość uderu energii min. 450 J) oraz filtrowanie zakłóceń EMI/RFI.Ochrona linii telekomunikacyjnej / sieciowej (złącze RJ11/RJ45 combo) z obsługą transmisji danych o prędkości do 1 Gbps.

Parametr	Charakterystyka (wymagania minimalne)
Komunikacja i zarządzanie	7. Wielofunkcyjny wyświetlacz LCD wskazujący stan pracy, poziom obciążenia, stan naładowania baterii, napięcia oraz ostrzeżenia/błędy. Porty komunikacyjne: USB (kompatybilny z HID) oraz port szeregowy RS-232. Współpraca z dedykowanym oprogramowaniem producenta do monitoringu i bezpiecznego zamykania systemów operacyjnych.
Obudowa i warunki pracy	8. Obudowa wolnostojąca (Tower) wykonana z trwałego tworzywa sztucznego. Wymiary maksymalne: ok. 100 × 355 × 281 mm (szer. × gł. × wys.), masa z bateriami ok. 10,4 kg. Poziom hałasu < 50 dBA (z odległości 1 m), temperatura pracy 0–40°C, wilgotność względna 0–90% (bez kondensacji).
Certyfikaty i gwarancja	9. Zgodność z normami CE, certyfikat Energy Star. Gwarancja producenta min. 24 miesiące.

VII. Switche zarządzalne do SUW i serwerowni

Typ I – Serwerownia 1szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Zarządzalny przełącznik sieciowy do montażu w szafie RACK 19" o wysokości 1U, przeznaczony do serwerowni (warstwa dystrybucji/dostępu). 2. Przełącznik wspierający system operacyjny RouterOS (licencja poziomu 5 oraz SwOS)
Porty	3. 48 × 10/100/1000 Mb/s Ethernet RJ-45. 4. 4 × SFP+ 10 Gb/s. 5. 2 × QSFP+ 40 Gb/s z możliwością bezpośredniego połączenia z innymi urządzeniami QSFP+. 6. 1 × port zarządzania Ethernet 10/100 Mb/s oraz port szeregowy RJ-45 (konsola).
Wydajność	7. Przepustowość całkowita (non-blocking) min. 168 Gb/s, pojemność przełączania min. 336 Gb/s. 8. Wydajność przekazywania pakietów min. 235 Mpps.
Procesor i pamięć	9. Procesor min. 650 MHz, pamięć RAM min. 64 MB, pamięć Flash min. 16 MB.
Zasilanie	10. Dwa wbudowane redundantne zasilacze AC 100–240 V; w razie awarii jednego zasilacza drugi przejmuje pracę. 11. Maksymalny pobór mocy do 60 W; w zestawie dwa przewody zasilające IEC.

Parametr	Charakterystyka (wymagania minimalne)
Funkcje zarządzania	12. Zarządzanie przez interfejs WWW, CLI (SSH, Telnet), konsolę szeregową oraz aplikację producenta. 13. Obsługa VLAN (802.1Q), agregacji łączy (LACP), protokołów Spanning Tree (STP/RSTP/MSTP), IGMP Snooping, kontroli dostępu (ACL) oraz mechanizmów QoS. 14. Obsługa SNMP, monitorowanie temperatury procesora i płytki oraz napięcia zasilania. 15. Możliwość pracy w trybie przełącznika warstwy 2 z funkcjami routingu (RouterOS).
Elementy montażowe	16. Uchwyty do montażu w szafie RACK 19" oraz zestaw śrub, nóżki i prowadnice na kable w zestawie. 17. Wymiary maks. 297 × 443 × 44 mm.
Warunki pracy i certyfikaty	18. Zakres temperatur pracy co najmniej od -20°C do +60°C. 19. Certyfikaty CE/RED, RoHS.

Typ II – SUWy – 3szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Kompaktowy zarządzalny przełącznik sieciowy 10 Gb/s przeznaczony do stacji uzdatniania wody (SUW) i niewielkich węzłów sieciowych; możliwość montażu w szafie RACK 19" (uchwyty w zestawie) lub jako urządzenie wolnostojące. 2. Obsługa systemów RouterOS (licencja poziomu 5) oraz SwOS (dual boot).
Porty	3. 8 × SFP+ 10 Gb/s. 4. 1 × 10/100/1000 Mb/s Ethernet RJ-45 (port zarządzania, z obsługą zasilania PoE-in). 5. Port szeregowy RS-232 oraz zacisk uziemienia.
Wydajność	6. Przepustowość całkowita (non-blocking) min. 81 Gb/s, pojemność przełączania min. 162 Gb/s.
Procesor i pamięć	7. Procesor dwurdzeniowy min. 800 MHz, pamięć RAM min. 512 MB, pamięć Flash min. 16 MB.
Zasilanie	8. Dwa wejścia zasilania: gniazdo DC 12–57 V oraz PoE-in (802.3af/at, 18–57 V). 9. Maksymalny pobór mocy do 33 W; zasilacz w zestawie.
Chłodzenie	10. Chłodzenie pasywne – bez wentylatorów (brak hałasu i gromadzenia kurzu), metalowa obudowa pełniąca funkcję radiatora.
Funkcje zarządzania	11. Zarządzanie przez interfejs WWW, CLI (SSH, Telnet) oraz konsolę szeregową.

Parametr	Charakterystyka (wymagania minimalne)
	12. Obsługa VLAN (802.1Q), agregacji łączy (LACP), protokołów Spanning Tree (STP/RSTP/MSTP), IGMP Snooping, kontroli dostępu (ACL) oraz mechanizmów QoS. 13. Obsługa SNMP oraz możliwość zdalnego zarządzania.
Elementy montażowe i wymiary	14. Uchwyty do montażu w szafie RACK 19" w zestawie. 15. Wymiary maks. 141 × 115 × 28 mm.
Warunki pracy i certyfikaty	16. Zakres temperatur pracy co najmniej od -40°C do +70°C – przystosowanie do pracy w trudniejszych warunkach (SUW). 17. Certyfikaty CE, RoHS.

VIII.Szafa Rack

Typ I – Serwerownia 1szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ i przeznaczenie	1. Szafa stojąca, teleinformatyczna i serwerowa 19", przeznaczona do montażu urządzeń telekomunikacyjnych, serwerów oraz systemów zasilania w centrach danych i serwerowniach.
Standard i wymiary	2. Standard montażowy: 19". Wysokość użytkowa: 42U.Wymiary zewnętrzne (szerokość × głębokość × wysokość): min. 800 × 1000 × (wysokość z cokołem/kółkami dostosowana do standardu 42U, ok. 2000–2050 mm).
Konstrukcja i nośność	3. Stabilna konstrukcja spawana/skręcana z wysokiej jakości stali malowanej proszkowo (kolor czarny, np. RAL 9005). Nośność statyczna szafy: min. 1000 kg. Przestrzeń 800 mm szerokości wyposażona w dodatkowe organizery kablowe / kanały kablowe ułatwiające pionowe prowadzenie kabli.
Drzwi i panele	4. Drzwi przednie: szklane (szkło hartowane) w stalowej ramie, z zamkiem kluczykowym, z możliwością zmiany strony otwierania (prawo/lewo), wentylowane po bokach lub perforowane w stopniu zapewniającym prawidłowy obieg powietrza.Drzwi tylne: stalowe, pełne lub perforowane (dwuskrzydłowe lub jednoskrzydłowe), z zamkiem kluczykowym.Panele boczne: demontowane panele stalowe wyposażone w zamki lub zatrzaski ułatwiające serwisowanie.
Szyny montażowe (Profil RACK)	5. 4 sztuki perforowanych profili montażowych 19" (2 z przodu, 2 z tyłu) z wyraźnie naniesioną skalą jednostek wysokości (U), z możliwością regulacji położenia w głębi szafy.

Parametr	Charakterystyka (wymagania minimalne)
Wentylacja i przepływ powietrza	6. Dach szafy przygotowany do montażu panelu wentylacyjnego (opcja z wentylatorami dachowymi) oraz przepusty kablowe w dachu i podłodze (górne i dolne płyty przepustowe).
Wypożyczenie dodatkowe i akcesoria	7. Szafa wyposażona w regulowane nóżki poziomujące oraz zestaw kół jezdnych z hamulcem ułatwiających pozycjonowanie. Komplet śrub montażowych (koszyczki, śruby, podkładki) – min. zestaw startowy.
Certyfikaty i gwarancja	8. Zgodność z normami teleinformatycznymi (np. EIA-310-D, IEC 60297-2, DIN 41494). Gwarancja producenta min. 24 miesiące.

TYP II – SUWy – 3szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ i przeznaczenie	1. Szafa teleinformatyczna w wersji uniwersalnej (przystosowana do montażu jako stojąca lub wisząca),
Standard i wymiary	2. Standard montażowy: 19". Wysokość użytkowa: 12U. 3. Wymiary zewnętrzne (szerokość × głębokość × wysokość): ok. 600 × 600 × (wysokość dostosowana do standardu 12U, ok. 640–650 mm ze stopkami/kółkami lub uchwytem ściennym).
Konstrukcja i nośność	4. Konstrukcja skręcana z blachy stalowej malowanej proszkowo (kolor czarny, np. RAL 9005). 5. Nośność szafy dostosowana do montażu wiszącego oraz stojącego (zgodnie ze specyfikacją producenta dla serii kompaktowych).
Drzwi i panele	6. Drzwi przednie: szklane (szkło hartowane) w stalowej ramie, z zamkiem kluczykowym, z możliwością zmiany strony otwierania (prawy/lewy). 7. Panele boczne: demontowane (zatraskowe/z zamkiem), ułatwiające dostęp serwisowy do wnętrza szafy i zamontowanych urządzeń.
Szyny montażowe (Profili RACK)	8. Perforowane profile montażowe 19" z możliwością regulacji głębokości montażu wewnątrz szafy, z czytelną skalą jednostek wysokości (U).
Wentylacja i przepływ powietrza	9. Przepusty kablowe umieszczone w górnej i dolnej płycie szafy, z możliwością montażu wentylatora chłodzącego w dachu.
Wypożyczenie dodatkowe	10. Zestaw montażowy (śruby, nakrętki klatkowe), zamek w drzwiach przednich; możliwość doposażenia w kółka jezdne lub nóżki poziomujące w przypadku zastosowania jako szafa stojąca.
Certyfikaty i gwarancja	11. Zgodność z normami branżowymi dla szaf 19". 12. Gwarancja producenta min. 24 miesiące.

IX. Agregat stacjonarny (20 kW) do SUW – 3szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Stacjonarny trójfazowy agregat prądotwórczy z silnikiem wysokoprężnym zasilany olejem napędowym, przystosowany do pracy ciągłej, przeznaczony do awaryjnego zasilania obiektu. 2. Napięcie wyjściowe 3 × 400 V / 230 V, częstotliwość 50 Hz.
Moc	3. Moc znamionowa prądnicy min. 20 kW (25 kVA). 4. Moc maksymalna (do 15 minut) min. 24 kW (30 kVA). 5. Prąd znamionowy min. 29 A na fazę.
Silnik	6. Silnik wysokoprężny (diesel), 4-cylindrowy, rzędowy, pojemność skokowa min. 3600 cm³, moc silnika min. 20 kW (44 KM). 7. Prędkość obrotowa 1500 obr./min, chłodzenie cieczą (chłodnica), wtrysk z pompą wtryskową, mechaniczna regulacja obrotów. 8. Silnik wolnossący, przystosowany do pracy ciągłej, rozruch elektryczny.
Prądnica	9. Prądnica synchroniczna, bezszczotkowa, samowzbudna, model klasy SLG-184F lub równoważny. 10. Praca w układzie trójfazowym 400 V oraz jednofazowym 230 V.
Gniazda wyjściowe	11. 230 V / 16 A, 12. 230 V / 32 A, 13. 400 V / 32 A.
Zbiornik paliwa i autonomia	14. Centralnie umieszczony zbiornik paliwa (pod silnikiem i prądnicą) umożliwiający pracę agregatu przez min. 10 godzin przy obciążeniu maksymalnym oraz min. 15 godzin przy obciążeniu 70%.
Współpraca z zasilaniem gwarantowanym	15. Agregat musi współpracować z zasilaczem awaryjnym UPS typu ON-LINE o mocy 10 kVA / 10 kW z trójfazowym wejściem 400 V. 16. Moc agregatu musi zapewniać zasilanie UPS-a wraz z ładowaniem jego akumulatorów oraz pozostałych odbiorników awaryjnych obiektu.
Gwarancja	17. Gwarancja producenta lub dostawcy zgodnie z warunkami oferty. 18. Instrukcja obsługi w języku polskim.

X. System monitorowania sieci OT / IDS dla OT

1. Przedmiotem zamówienia jest:
2. wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
3. dostawa licencji oraz sond sprzętowych,

4. udzielenie wsparcia dla administratorów Zamawiającego,
5. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie musi stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
 - a) pasywne monitorowanie sieci przemysłowej Zamawiającego,
 - b) automatyczne tworzenie graficznej mapy rzążeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
 - c) szczegółową inwentaryzację urządzeń,
 - d) automatyczne odzwierciedlenie połączeń komunikacyjnych,
 - e) informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
 - f) wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
 - g) budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
 - h) obsługę LLDP, CDP, CIP, SSDP.
10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS musi być oparty na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.

18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)
20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:
 - a) malware/"zero-day",
 - b) atak DOS/DDOS,
 - c) atak typu ATP,
 - d) spyware, skanowanie sieci,
 - e) zagrożenia Man-in-the-Middle,
 - f) anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
 - g) wykrywanie połączeń do innej sieci LAN/internet,
 - h) wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BROADCAST.
35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.

42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem baterijnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
45. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
49. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
50. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
51. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

Dostawa, wdrożenie.

1. Wykonawca dostarczy:
 - a) sondy sprzętowe w liczbie 1 szt. do monitorowania sieci przemysłowej dla każdego z SUW,
 - b) licencję wieczystą na system IDS nielimitowanej monitorowanych urządzeń,
 - c) usługi wsparcia serwisowego producenta systemu IDS na okres 36 miesięcy.
2. serwis producenta systemu IDS ma obejmować:
 - a) Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
 - b) Dostęp do nowych wersji systemu IDS.
 - c) Dostęp do aktualizacji i poprawek systemu IDS.
 - d) Dostęp do aktualizacji oprogramowania sond sprzętowych.
 - e) Wymianę uszkodzonych sond sprzętowych w razie awarii.
 - f) Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
 - g) Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
 - h) Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
3. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
4. Sprzęt serwerowy wraz z niezbędnym oprogramowaniem tj. jak system operacyjny, wirtualizator, itp. - zapewni Zamawiający.
5. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
6. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
7. Wykonawca przekaze Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
8. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi

testy sprawdzające prawidłowość jego wykonania i działania.

9. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
10. Wykonawca przeprowadzi instruktarz dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.
11. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

XI. Zakres wdrożenia infrastruktury IT i OT

Zakres według lokalizacji:

Lokalizacja	Dostawa i zakres
Serwerownia Zamawiającego	1 szafa RACK 42U; 1 UPS typu I (20 kVA / 18 kW); 1 UTM typu II; 1 switch typu I; 2 serwery z oprogramowaniem; 1 macierz; 1 komplet backupu. Centralny IDS oraz wdrożenie oprogramowania IT.
SUW Stefanków Działka 48/2	1 agregat 20 kW; 1 UPS typu II (1600 VA / 960 W); 1 szafa RACK 12U; 1 UTM typu I; 1 switch typu II; 1 sonda sprzętowa IDS. Pełny montaż i konfiguracja.
SUW Koziegłowy Działka 21	1 agregat 20 kW; 1 UPS typu II (1600 VA / 960 W); 1 szafa RACK 12U; 1 UTM typu I; 1 switch typu II; 1 sonda sprzętowa IDS. Pełny montaż i konfiguracja.
SUW Warpęsy Działka 140	1 agregat 20 kW; 1 UPS typu II (1600 VA / 960 W); 1 szafa RACK 12U; 1 UTM typu I; 1 switch typu II; 1 sonda sprzętowa IDS. Pełny montaż i konfiguracja.
SUW Jasieniec ul. Warecka Działki 104/1–104/3	Integracja istniejącej automatyki i SCADA firmy POSTER z Poznania z monitoringiem OT.
Oczyszczalnia ścieków w Jasieńcu, Kasztanowa 8, 05-604 Jasieniec	Integracja istniejącego SCADA firmy POSTER i komunikacji automatyki z centralnym monitoringiem OT.

Wdrożenie w serwerowni

1. Wykonawca złoży i ustawi szafę RACK 42U, zapewni połączenia ochronne, właściwą wentylację i dostęp serwisowy oraz zamontuje urządzenia, szyny, półki, listwy zasilające i organizery.
2. Wykonawca podłączy UPS typu I, skonfiguruje monitoring i uzgodniony sposób bezpiecznego wyłączania systemów. Dobierze zasilanie urządzeń i zabezpieczenia zgodnie z dokumentacją producentów.
3. Wykonawca uruchomi dwa serwery, systemy operacyjne, środowisko wirtualizacji i klastr. Wykona konfigurację sieci zarządzania, komunikacji klastra i pamięci masowej oraz integrację z istniejącą macierzą Zamawiającego.
4. NAS zostanie uruchomiony jako dodatkowy magazyn danych: konfiguracja dysków, przestrzeni, udziałów, uprawnień, monitorowania stanu i powiadomień, według uzgodnionego przeznaczenia. Nie należy utożsamiać go z istniejącą macierzą klastra.

5. Wykonawca skonfiguruje switch typu I i UTM typu II, plan adresacji, VLAN, segmentację, reguły dostępu, VPN do wskazanych obiektów, logowanie, NTP i dostęp administracyjny, w tym MFA w zakresie wymaganym przez OPZ.
6. Wykonawca aktywuje i skonfiguruje platformę EPP/EDR z CTEM oraz system zarządzania IT. Wdroży agentów, polityki, uprawnienia i powiadomienia na urządzeniach objętych licencjami. System zarządzania IT obejmuje co najmniej 10 stanowisk Windows i wszystkie serwery dostarczane w ramach postępowania;
7. Wykonawca uruchomi centralny IDS w środowisku wskazanym przez Zamawiającego, skonfiguruje użytkowników, źródła danych, obiekty OT, retencję, alarmy i raporty. Dane IDS pozostają w infrastrukturze Zamawiającego zgodnie z OPZ.
8. Wykonawca zintegruje kompletny system backupu ze środowiskiem klastrowym, obejmie ochroną minimum 5 VM i skonfiguruje harmonogramy, retencję, deduplikację, kompresję oraz ochronę kopii przed usunięciem lub zmianą. Repozytorium zapewnia minimum 8 TB przestrzeni użytkowej zgodnie z OPZ.
9. Wykonawca wykona i udokumentuje próbę backupu oraz odtworzenia co najmniej jednej kompletnej VM i jednego pliku. Przekaze procedurę odtwarzania i instruktaż obsługi.
10. Wykonawca zapewni transport, rozładunek, posadowienie UPSu, podłączenie, zabezpieczenia, uziemienie i przewody zasilające oraz sterownicze.
11. Przed montażem wykonawca zweryfikuje bilans mocy, prądy rozruchowe, kolejność załączania i zakres odbiorów zasilanych awaryjnie. Sprawdzi współpracę z UPS z agregatem.
12. Wykonawca zapewni opracowania projektowe oraz przeprowadzenie wymaganych dla wybranego rozwiązania uzgodnień, zgłoszeń i procedur uzyskania decyzji lub pozwoleń, wraz z kosztami objętymi zakresem zamówienia. Gdy wymagane jest działanie Zamawiającego jako właściciela lub inwestora, wykonawca przygotowuje dokumenty, a Zamawiający zapewni podpisy lub pełnomocnictwa.
13. Wykonawca przeprowadzi pomiary elektryczne, próby pod obciążeniem, test zaniku i powrotu zasilania oraz współpracy z agregatem. Prace elektryczne wykonają osoby z odpowiednimi kwalifikacjami.

Wdrożenie w SUW

Poniższe wymagania obowiązują oddzielnie w SUW Stefanków, SUW Koziegłowy i SUW Warpęsy. W każdej lokalizacji wykonawca uruchamia kompletny zestaw wskazany w OPZ

Agregat i układy zasilania

1. Wykonawca zapewni transport, rozładunek, posadowienie agregatu, wymagane podłoże lub fundament, podłączenie, automatykę SZR, zabezpieczenia, uziemienie i przewody zasilające oraz sterownicze. Układ musi zapobiegać podaniu napięcia z agregatu do sieci zasilającej.
2. Przed montażem wykonawca zweryfikuje bilans mocy, prądy rozruchowe, kolejność załączania i zakres odbiorów zasilanych awaryjnie.
3. Wykonawca zapewni opracowania projektowe oraz przeprowadzenie wymaganych dla wybranego rozwiązania uzgodnień, zgłoszeń i procedur uzyskania decyzji lub pozwoleń, wraz z kosztami objętymi zakresem zamówienia. Gdy wymagane jest działanie Zamawiającego jako właściciela lub inwestora, wykonawca przygotowuje dokumenty, a Zamawiający zapewni podpisy lub pełnomocnictwa.
4. Wykonawca przeprowadzi pomiary elektryczne, próby pod obciążeniem, test zaniku i powrotu zasilania oraz współpracy z UPS. Zapewni paliwo na uruchomienie i próby. Prace elektryczne wykonają osoby z odpowiednimi kwalifikacjami.

Szafa i urządzenia sieciowe

1. Wykonawca zamontuje szafę RACK 12U, UPS typu II, UTM typu I, switch typu II i sondę IDS. Zapewni wymagane zasilanie sondy i podtrzymanie zgodnie z OPZ, mocowania, wentylację, połączenia ochronne i oznaczenia.

2. Wykonawca skonfiguruje VLAN, porty, VPN do serwerowni, reguły dostępu, monitoring, synchronizację czasu i powiadomienia. Zapewni moduły SFP/SFP+, adaptory i okablowanie umożliwiające połączenie portów dostarczanych switchy z rzeczywistymi interfejsami urządzeń.
3. Wykonawca uruchomi sondy sprzętowej IDS w każdej z trzech SUW, kopię ruchu i analizę pasywną, bez zakłócania sterowania. Zweryfikuje widoczność urządzeń i zdarzeń w centralnym systemie oraz wykona testy alarmów.
4. Wykonawca zapewni niezbędny dostęp do Internetu na potrzeby VPN.

Integracja istniejących obiektów SUW i oczyszczalni ścieków Jasieniec

Obiekty posiada automatykę i oprogramowanie SCADA firmy POSTER z Poznania, powiadomienia SMS, lokalny monitoring wizyjny oraz agregat prądotwórczy.

1. Wykonawca obejmie monitoringiem IDS komunikację SCADA i urządzeń automatyki, zapewni konfigurację połączeń, źródeł kopii ruchu oraz niezbędnych elementów integracyjnych i licencji.
2. Integracja zachowa sterowanie procesem, transmisję danych, alarmy SMS, monitoring wizyjny i dotychczasową pracę zasilania awaryjnego.
3. Monitoring będzie pasywny i nie może zakłócać procesu oczyszczania, sterowania, alarmów ani komunikacji SCADA.
4. Wykonawca zweryfikuje zgodność oferowanego systemu z infrastrukturą obiektów, uzgodni sposób integracji i skoordynuje wymagane prace z dostawcą istniejącego SCADA, przy udziale Zamawiającego.
5. Dane, urządzenia i zdarzenia będą prezentowane w centralnym IDS z jednoznacznym przypisaniem do obiektu. Zakres obejmuje konfigurację powiadomień i raportowania, testy komunikacji oraz potwierdzenie zachowania istniejących funkcji.
6. Zamawiający udostępni posiadaną dokumentację, uzgodnione dostępy i możliwość przeprowadzenia prac. Integracja dotyczy monitorowania cyberbezpieczeństwa; nie oznacza zastąpienia systemów SCADA ani budowy wspólnego sterowania procesami.

Materiały odbiór i przekazanie

1. Cena musi zawierać materiały i prace niezbędne do wykonania określonego zakresu: przewody, moduły, złącza, zabezpieczenia, zasilacze, listwy, szyny, półki, uchwyty, organizery, przepusty i oznaczenia. Wykonawca wykona trasy kablowe, uszczelnienia i odtworzy naruszone powierzchnie oraz teren.
2. Harmonogram, przerwy i zmiany konfiguracji wymagają uzgodnienia. Przed zmianami Wykonawca zabezpieczy konfigurację i dane oraz przygotowuje sposób powrotu do poprzedniego stanu. Prace nie mogą powodować nieuzgodnionych przerw technologicznych.
3. Odbiór obejmuje serwerownię oraz pięć obiektów OT. Wykonawca prześle wyniki testów zasilania, VPN, segmentacji, IDS, ochrony i zarządzania IT, klastra, NAS oraz backupu i odtwarzania. Usunie usterki uniemożliwiające spełnienie OPZ.
4. Dokumentacja powykonawcza musi zawierać schematy elektryczne i sieciowe, adresację i VLAN, wykaz urządzeń i licencji, konfiguracje, protokoły pomiarów i testów, dokumenty dotyczące agregatów oraz instrukcje konserwacji i odtwarzania. Należy ją przekazać przed odbiorem, z zachowaniem terminu przewidzianego w OPZ dla IDS.
5. Wykonawca prześle Zamawiającemu konta właścicielskie i administracyjne, licencje oraz hasła bezpiecznym kanałem. Pozostawienie dostępu wykonawcy wymaga zgody. Zakres obejmuje instruktaż obsługi.