

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu prowadzonym w trybie otwartej procedury konkurencyjnej pn.
**„Wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa
dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o.,
w ramach projektu „Cyberbezpieczne Wodociągi”**

**CZĘŚĆ II - DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ
OPROGRAMOWANIA**

1. Przedmiotem niniejszego postępowania jest wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o., w ramach projektu „Cyberbezpieczne Wodociągi, poprzez realizację zadań technicznych - wzmacniających poziom cyberbezpieczeństwa systemów (część II zamówienia).
2. Zakres rzeczowy poszczególnych części określono szczegółowo w dalszej części OPZ. Realizacja zamówienia ma zapewnić osiągnięcie przez Zamawiającego celów i wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem oraz dostosowanie do wymagań wynikających z przepisów o krajowym systemie cyberbezpieczeństwa.

Przedmiotem zamówienia jest dostawa sprzętu oraz oprogramowania na potrzeby
**PRZEDSIĘBIORSTWA KOMUNALNEGO W TUCHOLI SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ.**

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

1. Całość oferowanego i dostarczanego sprzętu oraz oprogramowania IT musi być fabrycznie nowa.
2. Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, które wskazują lub mogłyby wskazywać na konkretnego producenta/dostawcę – nie stanowi to preferowania konkretnego wyrobu lub producenta/dostawcy lecz ma na celu jedynie wskazanie cech - parametrów technicznych, użytkowych i jakościowych nie gorszych od podanych w opisie. Należy to więc traktować jedynie jako pomoc w opisie przedmiotu zamówienia.
3. Jeżeli Wykonawca stwierdzi, że użyte w opisie parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy.

4. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w opisie, również dopuszcza się wykazanie normami równoważnymi w stosunku do tych wskazanych. Na Wykonawcy spoczywa ciężar wykazania „równoważności”. Wykonawca musi zaoferować spełniające min. takie wymagania i parametry techniczne, jak w opisie przedmiotu zamówienia. Wykonawca może zaoferować produkty o lepszych parametrach.
5. Dostarczone przedmioty zamówienia powinny być fabrycznie nowe, wykonane zgodnie z wymaganiami i normami mającymi zastosowanie do danego wyrobu, wolne od wad, odpowiadać normom jakościowym, określonym we właściwych aktach prawnych, posiadać aktualne aprobaty techniczne, gwarancje producenta oraz winny spełniać wszelkie wymagania przewidziane obowiązującymi przepisami dla tego typu wyrobów.
6. Zakres przedmiotu zamówienia obejmuje wykonanie instalacji, uruchomienie, wdrożenie oraz konfigurację sprzętu i systemów/licencji zgodnie z wymaganiami i zaleceniami Zamawiającego lub najlepszymi praktykami oraz doświadczeniem Dostawcy.
7. **Zamawiający wymaga, aby oferowane produkty ICT, usługi ICT lub procesy ICT:**
 - a) nie były objęte rekomendacją, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
 - b) nie były objęte decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka, wydaną na podstawie art. 67b ust. 15 ustawy o krajowym systemie cyberbezpieczeństwa.

**Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:
Zestawienie wymaganego sprzętu, oprogramowania i dokumentacji**

Lp.	Asortyment	Ilość
1.	Oprogramowanie typu EDR wraz z wdrożeniem	1 kpl.
2.	Serwer skonfigurowany w trybie HA z opcją wirtualizacji	2 szt.
3.	Serwer skonfigurowany w trybie autonomicznym z funkcją HA	1 szt.
4.	Macierz dyskowa	1 szt.
5.	Switch zarządzalny skonfigurowany w trybie HA	2 szt.
6.	Wdrożenie wszystkich systemów IT i OT	1 kpl.
7.	Urządzenia brzegowe/UTM router z wbudowanymi kontrolerami WiFi wraz z niezbędnymi licencjami	2 szt.
8.	Urządzenia brzegowe/UTM router wraz z niezbędnymi licencjami	3 szt.
9.	System do monitorowania infrastruktury i inwentaryzacji aktywów IT	1 kpl.
10.	Szafa RACK na serwery	1 kpl.
11.	Testy bezpieczeństwa sieci oraz serwisów www	1 kpl.
12.	Licencje wieczyste na system operacyjny dla serwerów	3 szt.

1. Oprogramowanie typu EDR wraz z wdrożeniem

Licencje

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową do dnia 31/12/2026.

Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. do dnia 31/12/2026 gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

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

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

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

Ilość stacji roboczych: 77

Ilość serwerów: 3

Ochrona punktów końcowych urządzeń komputerowych

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.

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

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 10
- Microsoft Windows 11
- macOS 15 "Sequoia"
- macOS 14 "Sonoma"
- macOS 13 "Ventura"

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

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

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

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

1. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.

3. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
 - dostęp do pliku;
 - tworzenie nowego procesu;
 - nawiązane połączenia sieciowe;
 - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. 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.
12. Dane zbierane przez agentów zainstalowanych na stacjach końcowych muszą być przechowywane i przetwarzane wyłącznie na terytorium Unii Europejskiej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
 - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
 - Data i czas wystąpienia podejrzanych zdarzeń.
 - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.

- Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
 - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
 - Poziom ryzyka, określający istotność danej detekcji.
 - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. 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).
 21. 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).
 22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
 23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
 24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
 25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
 26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
 27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
 28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
 29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
 30. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
 31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
 32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
 33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
 34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
 35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
 36. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
 37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.

38. 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.
39. 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. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
40. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
41. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
42. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
43. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
44. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
45. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
46. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
47. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
48. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
49. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
50. 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.
51. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
52. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
54. 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.
55. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
56. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
57. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
58. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
59. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.

60. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
61. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
62. 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.
63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
64. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
65. 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).
66. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
67. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
68. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
69. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
70. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
71. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
72. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przysyłania podejrzanych plików do dodatkowej analizy przez producenta.
73. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
74. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
75. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
76. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
77. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
78. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
79. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.

80. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
81. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
82. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skrypty ActiveX i pobierane pliki.
83. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
84. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
85. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
87. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
88. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
90. 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.
91. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
92. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
93. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
94. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
95. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
96. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
97. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
98. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
99. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
100. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

101. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
102. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
103. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
104. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
105. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
106. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na stronę producenta aplikacji.
107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
108. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
109. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
110. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
111. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
112. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
113. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
114. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
115. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
116. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
117. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
118. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
119. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
120. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.

121. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
122. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
123. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
124. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
125. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
126. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
127. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
128. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
129. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
130. 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.
131. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
132. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
133. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
134. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
135. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
136. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
137. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
138. 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.
139. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
140. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
141. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN

142. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
143. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
144. Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).
145. Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia 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. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamiania o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego połączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.

17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji

Rozszerzone wsparcie serwisowe

System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia 31/12/2026.

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

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Przygotowanie do zdalnej konfiguracji.
- Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Wymagania dotyczące wsparcia technicznego i serwisu

W celu zapewnienia odpowiedniego poziomu jakości, bezpieczeństwa i ciągłości świadczonych usług podmiot odpowiedzialny za świadczenie wsparcia technicznego dla oferowanego rozwiązania musi posiadać:

1. certyfikat zgodności systemu zarządzania jakością z normą **ISO 9001:2015** lub normą równoważną;
2. certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z normą **ISO/IEC 27001:2022** lub normą równoważną.

Zakres certyfikacji podmiotu świadczącego wsparcie musi obejmować świadczenie usług wsparcia technicznego, serwisowych lub utrzymaniowych oraz usług związanych z bezpieczeństwem teleinformatycznym lub cyberbezpieczeństwem, odpowiednio do zakresu realizowanego zamówienia.

Obsługa zgłoszeń serwisowych

Podmiot świadczący wsparcie techniczne zapewni możliwość dokonywania zgłoszeń serwisowych przez Zamawiającego **24 godziny na dobę, 7 dni w tygodniu (24x7)**, co najmniej za pośrednictwem:

- a) dedykowanego internetowego systemu obsługi zgłoszeń serwisowych (portalu serwisowego);
- b) telefonicznej infolinii serwisowej.

Obsługa zgłoszeń oraz komunikacja z Zamawiającym, zarówno poprzez portal serwisowy, jak i infolinię, musi być dostępna **w języku polskim**.

Dokumenty potwierdzające

Wykonawca przedłoży dokument producenta oferowanego rozwiązania, jego autoryzowanego dystrybutora lub autoryzowanego podmiotu świadczącego wsparcie techniczne, potwierdzający gotowość świadczenia na rzecz Zamawiającego wymaganego wsparcia technicznego przez okres określony w dokumentacji zamówienia.

Dokument powinien zawierać lub wskazywać co najmniej:

- nazwę podmiotu odpowiedzialnego za świadczenie wsparcia;
- adres internetowego portalu obsługi zgłoszeń serwisowych;

- numer telefonicznej infolinii serwisowej;
- potwierdzenie dostępności przyjmowania zgłoszeń w trybie 24x7;
- potwierdzenie możliwości obsługi zgłoszeń w języku polskim.

Podmiot świadczący wsparcie techniczne musi posiadać ważne certyfikaty **ISO 9001:2015 oraz ISO/IEC 27001:2022 lub równoważne**, w zakresie odpowiadającym wymaganiom określonym powyżej.

W przypadku zaoferowania certyfikatu równoważnego Wykonawca zobowiązany jest wykazać, że certyfikat potwierdza funkcjonowanie systemu zarządzania odpowiadającego wymaganiom właściwej normy wskazanej przez Zamawiającego.

W ramach usługi Wykonawca przeprowadzi kompleksowe wdrożenie rozwiązania EDR, obejmujące przygotowanie, konfigurację, instalację oraz uruchomienie systemu ochrony, wykrywania i reagowania na zagrożenia na urządzeniach końcowych Zamawiającego.

Zakres wdrożenia obejmuje w szczególności:

1. **Analizę środowiska Zamawiającego** oraz przygotowanie planu wdrożenia rozwiązania EDR, z uwzględnieniem liczby i rodzaju chronionych urządzeń końcowych oraz istniejących mechanizmów bezpieczeństwa.
2. **Konfigurację środowiska zarządzania**, w tym:
 - utworzenie i konfigurację struktury organizacyjnej,
 - konfigurację kont i uprawnień administracyjnych,
 - konfigurację polityk bezpieczeństwa,
 - przygotowanie grup urządzeń i profili konfiguracyjnych.
3. **Instalację i uruchomienie agentów EDR** na wskazanych przez Zamawiającego stacjach roboczych i/lub serwerach, z wykorzystaniem odpowiedniej metody wdrożenia, w tym w szczególności instalacji zdalnej, skryptów instalacyjnych, narzędzi do centralnego zarządzania lub innych uzgodnionych metod.
4. **Konfigurację monitorowania aktywności urządzeń końcowych**, obejmującego w szczególności analizę procesów, aktywności systemowej, zachowań aplikacji oraz innych zdarzeń związanych z potencjalnymi zagrożeniami. Dane telemetryczne powinny być przekazywane do centralnego środowiska zarządzania w celu analizy i korelacji zdarzeń.
5. **Konfigurację mechanizmów wykrywania zagrożeń**, w tym:
 - wykrywania podejrzanych i złośliwych zachowań,
 - wykrywania zaawansowanych zagrożeń i prób ataków,
 - analizy zależności pomiędzy powiązаныmi zdarzeniami bezpieczeństwa,
 - konfiguracji poziomów i sposobów reagowania na wykryte incydenty.
6. **Konfigurację mechanizmów reagowania na incydenty**, w tym, w zakresie dostępnych funkcjonalności rozwiązania:
 - izolację urządzenia końcowego od sieci,
 - zatrzymywanie lub blokowanie złośliwych procesów,
 - podejmowanie działań ograniczających skutki incydentu,
 - obsługę i zmianę statusu wykrytych zdarzeń,
 - dokumentowanie podjętych działań administracyjnych i reakcji na incydenty.
7. **Konfigurację alertów i powiadomień** dotyczących wykrytych zagrożeń oraz zdarzeń bezpieczeństwa, zgodnie z wymaganiami Zamawiającego.
8. **Konfigurację zasad wykluczeń**, jeżeli okaże się to niezbędne dla prawidłowego funkcjonowania systemów i aplikacji Zamawiającego, z zachowaniem zasady minimalizacji zakresu wyłączeń.

9. **Weryfikację poprawności działania wdrożonego rozwiązania**, obejmującą co najmniej:

- o sprawdzenie komunikacji agentów z centralnym systemem zarządzania,
- o weryfikację poprawności raportowania zdarzeń,
- o weryfikację działania skonfigurowanych polityk bezpieczeństwa,
- o sprawdzenie poprawności generowania alertów,
- o weryfikację możliwości podjęcia działań reakcyjnych.

10. **Przeprowadzenie testów powdrożeniowych** oraz usunięcie ewentualnych nieprawidłowości ujawnionych podczas testów.

11. **Przeprowadzenie instruktażu dla administratorów Zamawiającego** w zakresie:

- obsługi konsoli zarządzającej,
- monitorowania stanu chronionych urządzeń,
- analizy alertów i zdarzeń,
- obsługi incydentów bezpieczeństwa,
- podejmowania działań reakcyjnych,
- zarządzania politykami bezpieczeństwa.

Wdrożenie uznaje się za zakończone po prawidłowym zainstalowaniu i uruchomieniu agentów EDR na urządzeniach objętych wdrożeniem, uzyskaniu komunikacji z centralną konsolą zarządzającą, przeprowadzeniu testów funkcjonalnych.

2. Serwer skonfigurowany w trybie HA z opcją wirtualizacji

Serwer powinien spełniać następujące wymagania:

Lp.	Parametr	Opis
1	Obudowa	- obudowa typu rack o wysokości nie większej niż 2U z min. 4 zatokami na dyski 2.5/3.5 cala hot-swap - wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania przez użytkownika własnego dysku bez konieczności zakupu dodatkowej ramki
2	Płyta główna	- jednoprocessorowa serwerowa z obsługą modułu TPM, obsługująca procesory serii Xeon® Scalable Processors generacji 4 i 5, min. 8 złączy DIMM, zintegrowana konsola zdalnego zarządzania - płyta musi posiadać możliwość instalacji dedykowanej, wewnętrznej pamięci M.2 SSD SATA przeznaczonej dla wirtualizatora (niezależne od dysków twardych)
3	Procesory	- zainstalowany 1 procesor, nie mniej niż 12 rdzeniowy i 24 wątkowy o prędkości taktowania co najmniej 2,0GHz i pamięci podręcznej cache nie mniejszej niż 30MB - osiągający w teście PassMark - CPU Mark min. 25000 punktów (wynik na dzień 30/06/2026)
4	Pamięć RAM	- zainstalowane min. 64 GB pamięci RAM typu DDR5 ECC - wsparcie dla technologii SDDC, Mirrored Channel Mode, - wsparcie dla konfiguracji pamięci w trybie Rank Sparing
5	Kontrolery dyskowe	- zainstalowany kontroler macierzy SAS/SATA umożliwiający konfigurację dysków w technologii RAID (minimum 8GB pamięci podręcznej cache kontrolera) - zainstalowany kontroler RAID 2x NVMe/SATA M-Key M.2

		(sprzętowy kontroler Hybrid NVMe/SATA 2x M.2)
6	Dyski twarde	- zainstalowane min. 2 dyski o pojemności nie mniejszej niż 960GB, PCIe NVMe, M.2, - zainstalowane min. 2 dyski o łącznej pojemności nie mniejszej niż 16TB, 3.5 cala, SATA III, 6 Gbit/s, 7200rpm
7	Kontrolery LAN	- minimum 4 porty Ethernet na serwer, w tym 2 × 10GbE, dopuszcza się realizację wymaganej liczby portów poprzez łączne wykorzystanie interfejsów zintegrowanych z płytą główną serwera lub dedykowanym modulem sieciowym niewykorzystującym standardowych gniazd PCIe oraz interfejsów zainstalowanych na kartach rozszerzeń PCIe - interfejsy muszą umożliwiać konfigurację redundantnych połączeń sieciowych oraz co najmniej dwóch niezależnych ścieżek komunikacji z macierzą dyskową
8	Porty	- zintegrowana karta graficzna ze złączem VGA - min. 6x USB, w tym min. 4x USB w standardzie 3.0
9	Zasilanie	- dwa zasilacze hot-plug o mocy min. 600W
10	Zarządzanie	- niezależna od zainstalowanego systemu operacyjnego dedykowana karta zarządzająca z dostępem przez dedykowany port RJ-45 Gigabit Ethernet zgodna z IPMI 2.0
11	Obsługiwane systemy operacyjne	- wsparcie dla systemów operacyjnych Windows i Linux - dostawa wraz z serwerem oprogramowania do wirtualizacji środowiska IT umożliwiającego uruchomienie wirtualnych systemów operacyjnych (linux, windows) na serwerze w klastrze
12	Oprogramowanie	- Microsoft Windows Server 2025 Standard lub równoważny - licencja obejmująca wszystkie fizyczne rdzenie procesorowe dostarczonego serwera, z uwzględnieniem minimalnych wymagań licencyjnych producenta
13	Inne wymagania	- zintegrowany z płytą lub procesorem moduł TPM
14	Gwarancja	- gwarancja producenta minimum 3 lata, z możliwością zgłaszania awarii 24×7×365 oraz świadczeniem serwisu w miejscu instalacji urządzenia, z czasem reakcji serwisu nie dłuższym niż następny dzień roboczy (NBD) od skutecznego zgłoszenia awarii - serwer musi być objęty przez cały okres gwarancji wsparciem technicznym producenta świadczonym w trybie 24×7×365, z możliwością całodobowego zgłaszania awarii - dyski muszą być objęte 36 miesięczną gwarancją producenta, - zepsute nośniki pozostają własnością zamawiającego
15	Dokumentacja, inne	- wszystkie elementy dostarczonego sprzętu muszą być fabrycznie nowe (nieużywane) i muszą pochodzić z oficjalnego kanału dystrybucji na rynek polski - wszystkie podzespoły, z których zbudowane są oferowane serwery, muszą pochodzić od producenta serwera lub być przez niego certyfikowane i dopuszczone do stosowania w oferowanym modelu serwera - wymagane certyfikaty PN-EN ISO 9001:2015, PN-EN

		ISO14001:2015 oraz PN-ISO/IEC 27001:2014 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis - wszystkie podzespoły muszą być objęte gwarancją producenta serwera - status, zakres i okres gwarancji muszą być możliwe do zweryfikowania na podstawie numeru seryjnego urządzenia w systemie producenta lub zostać potwierdzone dokumentem gwarancyjnym producenta
--	--	--

3. Serwer skonfigurowany w trybie autonomicznym z funkcją HA

Serwer powinien spełniać następujące wymagania:

Lp.	Parametr	Opis
1	Obudowa	- obudowa typu rack o wysokości nie większej niż 2U z min. 4 zatokami na dyski 2.5/3.5 cala hot-swap - wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania przez użytkownika własnego dysku bez konieczności zakupu dodatkowej ramki
2	Płyta główna	- jednoprocessorowa serwerowa z obsługą modułu TPM, obsługująca procesory serii Xeon® Scalable Processors generacji 4 i 5, min. 8 złączy DIMM, zintegrowana konsola zdalnego zarządzania - płyta musi posiadać możliwość instalacji dedykowanej, wewnętrznej pamięci M.2 SSD SATA przeznaczonej dla wirtualizatora (niezależne od dysków twardych)
3	Procesory	- zainstalowany 1 procesor, nie mniej niż 12 rdzeniowy i 24 wątkowy o prędkości taktowania co najmniej 2,0GHz i pamięci podręcznej cache nie mniejszej niż 30MB - osiągający w teście PassMark - CPU Mark min. 25000 punktów (wynik na dzień 30/06/2026)
4	Pamięć RAM	- zainstalowane min. 32 GB pamięci RAM typu DDR5 ECC - wsparcie dla technologii SDDC, Mirrored Channel Mode, - wsparcie dla konfiguracji pamięci w trybie Rank Sparing
5	Kontrolery dyskowe	- zainstalowany kontroler macierzy SAS/SATA umożliwiający konfigurację dysków w technologii RAID (minimum 8GB pamięci podręcznej cache kontrolera) - zainstalowany kontroler RAID 2x NVMe/SATA M-Key M.2 (sprzętowy kontroler Hybrid NVMe/SATA 2x M.2)
6	Dyski twarde	- zainstalowane min. 2 dyski o pojemności nie mniejszej niż 480GB, PCIe NVMe, M.2
7	Kontrolery LAN	- minimum 2 porty Ethernet na serwer, w tym 2 × 10GbE, dopuszcza się realizację wymaganej liczby portów poprzez łączne wykorzystanie interfejsów zintegrowanych z płytą główną serwera lub dedykowanym modulem sieciowym niewykorzystującym standardowych gniazd PCIe oraz interfejsów zainstalowanych na kartach rozszerzeń PCIe
8	Porty	- zintegrowana karta graficzna ze złączem VGA - min. 6x USB, w tym min. 4x USB w standardzie 3.0

9	Zasilanie	- dwa zasilacze hot-plug o mocy min. 600W
10	Zarządzanie	- niezależna od zainstalowanego systemu operacyjnego dedykowana karta zarządzająca z dostępem przez dedykowany port RJ-45 Gigabit Ethernet zgodna z IPMI 2.0
11	Obsługiwane systemy operacyjne	- wsparcie dla systemów operacyjnych Windows i Linux - dostawa wraz z serwerem oprogramowania do wirtualizacji środowiska IT umożliwiającego uruchomienie wirtualnych systemów operacyjnych (linux, windows) na serwerze w klastrze
12	Oprogramowanie	- Microsoft Windows Server 2025 Standard lub równoważny - licencja obejmująca wszystkie fizyczne rdzenie procesorowe dostarczonego serwera, z uwzględnieniem minimalnych wymagań licencyjnych producenta
13	Inne wymagania	- zintegrowany z płytą lub procesorem moduł TPM
14	Gwarancja	- gwarancja producenta minimum 3 lata, z możliwością zgłaszania awarii 24×7×365 oraz świadczeniem serwisu w miejscu instalacji urządzenia, z czasem reakcji serwisu nie dłuższym niż następny dzień roboczy (NBD) od skutecznego zgłoszenia awarii - serwer musi być objęty przez cały okres gwarancji wsparciem technicznym producenta świadczonym w trybie 24×7×365, z możliwością całodobowego zgłaszania awarii - dyski muszą być objęte 36 miesięczną gwarancją producenta, - zepsute nośniki pozostają własnością zamawiającego
15	Dokumentacja, inne	- wszystkie elementy dostarczonego sprzętu muszą być fabrycznie nowe (nieużywane) i muszą pochodzić z oficjalnego kanału dystrybucji na rynek polski - wszystkie podzespoły, z których zbudowane są oferowane serwery, muszą pochodzić od producenta serwera lub być przez niego certyfikowane i dopuszczone do stosowania w oferowanym modelu serwera - wymagane certyfikaty PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis - wszystkie podzespoły muszą być objęte gwarancją producenta serwera - status, zakres i okres gwarancji muszą być możliwe do zweryfikowania na podstawie numeru seryjnego urządzenia w systemie producenta lub zostać potwierdzone dokumentem gwarancyjnym producenta

4. Macierz dyskowa

Lp.	Parametr	Minimalne wymaganie
1	Typ urządzenia	Macierz dyskowa SAN przeznaczona do współdzielenia zasobów dyskowych przez minimum dwa serwery fizyczne
2	Obudowa	Rack 19", wysokość maksymalnie 2U
3	Kontrolery	Minimum 2 niezależne kontrolery macierzy

Lp.	Parametr	Minimalne wymaganie
4	Tryb pracy	Kontrolery pracujące w architekturze Active-Active, umożliwiającej jednoczesną pracę obu kontrolerów
5	Odporność na awarię	Awaria pojedynczego kontrolera nie może powodować utraty dostępu serwerów do danych
6	Failover	Automatyczne przejęcie obsługi zasobów/ścieżek w przypadku awarii jednego z kontrolerów
7	Wymiana kontrolerów	Możliwość wymiany uszkodzonego kontrolera bez konieczności wyłączania całej macierzy
8	Zatoki dyskowe	Minimum 12 zatok na dyski
9	Typ dysków	Obsługa dysków klasy enterprise SAS HDD i/lub SAS SSD
10	Hot-swap	Dyski wymienne podczas pracy urządzenia
11	Dostarczone dyski	Minimum 5 × 8 TB SAS HDD klasy enterprise, przeznaczonych i certyfikowanych/wspieranych przez producenta oferowanej macierzy
12	Prędkość dysków	Minimum 7200 obr./min dla HDD
13	Konfiguracja RAID	4 × 8 TB w RAID
14	Hot Spare	1 × 8 TB jako dedykowany lub globalny Hot Spare
15	Pojemność RAW	Minimum 40 TB z zainstalowanych 5 dysków
16	Pojemność RAID	Dla 4 × 8 TB RAID 5: około 24 TB + 8 TB Hot Spare Dla 4 × 8 TB RAID 6: około 16 TB + 8 TB Hot Spare
17	RAID	Obsługa co najmniej RAID 1, RAID 5, RAID 6 i RAID 10
18	Hot Spare	Obsługa automatycznego wykorzystania dysku zapasowego po awarii dysku należącego do RAID
19	Odbudowa RAID	Automatyczna odbudowa macierzy po wykorzystaniu dysku Hot Spare
20	Interfejs hostów	Minimum 10 Gb/s iSCSI lub 12 Gb/s SAS, zależnie od zaoferowanego wariantu macierzy (serwery muszą mieć zgodny interfejs z wariantem zaoferowanej macierzy). Połączenie serwerów z macierzą musi być realizowane bezpośrednio, bez konieczności stosowania dodatkowych przełączników SAN/LAN.
21	Redundancja połączeń	Każdy serwer musi posiadać redundantne ścieżki dostępu do macierzy poprzez oba kontrolery Minimum 4 porty Ethernet przeznaczone do komunikacji iSCSI z serwerami, po minimum 2 porty na każdy kontroler.
22	Multipathing	Obsługa wielościeżkowego dostępu do zasobów – MPIO/ALUA lub rozwiązania równoważnego
23	Liczba hostów	Możliwość jednoczesnego podłączenia minimum 2 serwerów
24	LUN	Możliwość tworzenia i udostępniania wielu logicznych jednostek LUN
25	Zarządzanie przestrzenią dyskową	Obsługa Thin Provisioning lub rozwiązania równoważnego
26	Snapshot	Obsługa wykonywania migawek wolumenów/LUN
27	Rozbudowa	Możliwość zwiększenia pojemności macierzy przez instalację kolejnych dysków i/lub podłączenie półki rozszerzającej
28	Zasilanie	Minimum 2 redundantne zasilacze
29	Hot-swap PSU	Możliwość wymiany zasilacza bez wyłączania macierzy

Lp.	Parametr	Minimalne wymaganie
30	Chłodzenie	Redundantny system chłodzenia
31	Zarządzanie	Zarządzanie macierzą przez interfejs graficzny WWW
32	Monitoring	Monitorowanie stanu kontrolerów, dysków, RAID, zasilaczy, wentylatorów oraz interfejsów komunikacyjnych
33	Powiadomienia	Automatyczne powiadamianie administratora o awariach lub zdarzeniach wymagających interwencji
34	Wirtualizacja	Wsparcie dla Microsoft Windows Server i Hyper-V
35	Klaster	Macierz musi być przeznaczona do udostępniania współdzielonej pamięci masowej dla klastra wysokiej dostępności
36	Okablowanie	W komplecie wszystkie niezbędne przewody/transceivery wymagane do redundantnego podłączenia dwóch dostarczanych serwerów
37	Szyny	Komplet szyn do montażu w szafie Rack 19"
38	Gwarancja	Gwarancja producenta minimum 3 lata NBD on-site (na miejscu u klienta) z możliwością zgłaszania awarii 24×7×365. Dyski muszą być objęte 36 miesięczną gwarancją producenta. Zepsute nośniki pozostają własnością zamawiającego.
39	Inne	Wszystkie podzespoły, z których zbudowana jest macierz, muszą pochodzić od producenta macierzy lub być przez niego certyfikowane i dopuszczone do stosowania w oferowanym modelu macierzy. Wszystkie podzespoły muszą być objęte gwarancją producenta macierzy.

5. Switch zarządzalny skonfigurowany w trybie HA

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej (**switchy zarządzalnych 48-portowych skonfigurowanych w trybie HA**). Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

1. 48 porty GE RJ-45.
2. 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).

- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Centralne zarządzanie konfiguracją urządzenia
- Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
- Centralne zarządzanie sieciami VLAN.
- Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
- Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
- Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.

Musi być możliwe redundantne połączenie z elementami zarządzającymi.

W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta **do dnia 31.12.2026**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wymagania dotyczące kwalifikacji personelu Wykonawcy

Wykonawca realizujący przedmiot zamówienia zobowiązany jest dysponować personelem posiadającym odpowiednią wiedzę, doświadczenie i kwalifikacje w zakresie projektowania, wdrażania, konfiguracji, administracji oraz utrzymania oferowanych rozwiązań bezpieczeństwa teleinformatycznego.

Wykonawca wykaże, że osoby skierowane do realizacji zamówienia posiadają łącznie aktualne certyfikaty producenta oferowanego rozwiązania lub certyfikaty równoważne, potwierdzające kompetencje co najmniej w następujących obszarach:

- a) **Bezpieczeństwo sieci (Network Security – NS)** – obejmujące co najmniej konfigurację, administrację i zabezpieczanie infrastruktury sieciowej, zapór sieciowych klasy NGFW/UTM, mechanizmów kontroli dostępu, VPN oraz systemów ochrony przed zagrożeniami sieciowymi;
- b) **Operacje bezpieczeństwa (Security Operations – SO)** – obejmujące co najmniej monitorowanie zdarzeń bezpieczeństwa, identyfikację i analizę zagrożeń, analizę incydentów oraz reagowanie na zdarzenia i incydenty bezpieczeństwa;
- c) **Secure Access Service Edge (SASE)** – obejmujące co najmniej projektowanie, konfigurację i administrację rozwiązaniami bezpiecznego dostępu do zasobów lokalnych i chmurowych, z uwzględnieniem mechanizmów kontroli dostępu oraz ochrony użytkowników;
- d) **Bezpieczeństwo chmury publicznej (Public Cloud Security – PCS)** – obejmujące co najmniej projektowanie, konfigurację, administrację lub zabezpieczanie środowisk i usług wykorzystujących chmurę publiczną.

Równoważność certyfikatów

Zamawiający dopuszcza certyfikaty równoważne.

Za certyfikat równoważny Zamawiający uzna certyfikat wydany przez producenta oferowanego rozwiązania, podmiot przez niego autoryzowany lub niezależną organizację certyfikującą, który potwierdza wiedzę i kompetencje w zakresie odpowiadającym wymaganiom określonym dla danego obszaru.

Certyfikat równoważny nie musi posiadać identycznej nazwy, oznaczenia, struktury poziomów ani ścieżki certyfikacyjnej jak certyfikaty innych producentów. O równoważności decyduje zakres potwierdzonych kompetencji, a nie nazwa certyfikatu.

W przypadku przedstawienia certyfikatu równoważnego Wykonawca przedstawi dokument lub informację umożliwiającą Zamawiającemu weryfikację zakresu certyfikacji, np. opis programu certyfikacyjnego, zakres egzaminu, odnośnik do oficjalnej dokumentacji podmiotu certyfikującego lub inny równoważny dokument.

Sposób spełnienia wymagań

Zamawiający dopuszcza, aby wymagane kompetencje były spełnione łącznie przez zespół osób skierowanych do realizacji zamówienia. Nie wymaga się, aby jedna osoba posiadała wszystkie wskazane certyfikaty.

Jedna osoba może jednocześnie potwierdzać spełnienie wymagań w więcej niż jednym obszarze. Certyfikaty powinny być aktualne na dzień wymagany dokumentacją postępowania, o ile dany program certyfikacyjny przewiduje okres ich ważności.

Na żądanie Zamawiającego Wykonawca przedstawi dokumenty umożliwiające weryfikację ważności i autentyczności wskazanych certyfikatów.

6. Wdrożenie wszystkich systemów IT i OT

Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie urządzenia oraz oprogramowanie na miejscu u Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym, uzgodnionym i zaakceptowanym przez Zamawiającego.

Projekt techniczny ma polegać na utworzeniu klastra składającego się z 2 serwerów i macierzy. W przypadku awarii jednego z urządzeń, drugie urządzenie ma automatycznie przejąć pracę pierwszego.

Systemy mają posiadać układ, który umożliwi szyfrowanie dysków twardych, co w przypadku dostępu osób trzecich do środowiska uniemożliwi odczyt danych. Macierz i serwery mają zapewnić wydajność oraz wymaganą pojemność dla usług i oprogramowania użytkowników.

Zamawiający wymaga dostarczenia wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (szafa rack, przewody krosowe, osprzęt montażowy).

Wykonawca po zainstalowaniu wszystkich dostarczonych urządzeń opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów. Dokumentacja powykonawcza będzie zawierała szczegółowe opisy zastosowanych rozwiązań oraz procedurę uruchomienia środowiska po awarii.

Wszystkie dostarczone urządzenia zostaną podłączone i skonfigurowane zgodnie z aktualną wiedzą techniczną i zaleceniami producenta przez certyfikowanego inżyniera dostarczonego sprzętu (*certyfikat do wglądu w siedzibie Zamawiającego*).

Wykonawca opracuje plan szkolenia z powyższego zakresu. Szkolenie w ramach przedmiotowego postępowania powinno w szczególności uwzględniać uwarunkowania montażu, instalacji i konfiguracji sprzętu w infrastrukturze Zamawiającego i jej użytkowania oraz obsługę kontrolera domeny.

Szkolenie ma zostać przeprowadzone w języku polskim przez certyfikowanego inżyniera dostarczonego sprzętu (*certyfikat do wglądu w siedzibie Zamawiającego*), który posiada odpowiednią wiedzę i przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań.

Opis

Przedmiotem zamówienia są usługi wdrożenia dostarczonych rozwiązań sprzętowych oraz oprogramowania w obszarze cyberbezpieczeństwa, funkcjonujących w środowiskach IT i OT Zamawiającego.

Zakres zamówienia obejmuje instalację, konfigurację, integrację oraz uruchomienie infrastruktury, a także przygotowanie jej do pracy produkcyjnej zgodnie z wymaganiami Zamawiającego.

Zakres infrastruktury objętej wdrożeniem

1.1 Infrastruktura sieciowa

- Serwery fizyczne klasy enterprise – 2 sztuki,
 - Stworzenie klastra HA,
- Macierz dyskowa klasy enterprise – 1 sztuka,
 - Montaż w szafie RACK 19”,
 - Przystosowanie do pracy ciągłej.
- Dyski klasy enterprise przeznaczone do pracy w trybie 24/7,
- Szafa teleinformatyczna RACK:
 - Standard 19”,
 - Wysokość 42U,
 - Głębokość 1000 mm,
 - Szerokość 600 mm,
 - Wyposażona w system kontroli temperatury (termostat).
 - Istniejące zasilanie awaryjne UPS.

1.2 Infrastruktura sieciowa i bezpieczeństwa

- Urządzenia klasy zapór sieciowych (NGFW/UTM),
- Zarządzalne przełączniki sieciowe.

1.3 Systemy uwierzytelniania

- Sprzętowe mechanizmy uwierzytelniania wieloskładnikowego (MFA):

1.4 Oprogramowanie

- System ochrony stacji końcowych
- System wykonywania kopii zapasowych (backup),
- System archiwizacji danych,
- System audytu i zgodności,
- Rozwiązania open source wykorzystane w środowiskach IT i OT.

Zakres prac wdrożeniowych

2.1 Przygotowanie do wdrożenia

- Analiza środowiska Zamawiającego,
- Opracowanie szczegółowego planu wdrożenia,
- Uzgodnienie harmonogramu prac,
- Identyfikacja zależności oraz ryzyk wdrożeniowych.

2.2 Instalacja fizyczna

- Montaż urządzeń w szafie RACK,
- Podłączenie zasilania (w tym zasilania redundantnego),
- Organizacja i oznakowanie okablowania,
- Weryfikacja warunków środowiskowych (temperatura, wentylacja, zasilanie).

3.3 Konfiguracja infrastruktury

- Konfiguracja serwerów i macierzy,
- Konfiguracja urządzeń sieciowych,
- Implementacja segmentacji sieci (VLAN),
- Konfiguracja usług sieciowych.

3.4 Wdrożenie systemów bezpieczeństwa

- Konfiguracja zapór sieciowych, systemów VPN oraz IPS/IDS,
- Wdrożenie i konfiguracja systemów ochrony endpointów,
- Konfiguracja uwierzytelniania wieloskładnikowego,
- Wdrożenie polityk bezpieczeństwa.

3.5 Wdrożenie systemów backupu i archiwizacji

- Konfiguracja polityk wykonania kopii zapasowych,
- Konfiguracja harmonogramów backupu,
- Wdrożenie polityk retencji danych,
- Konfiguracja archiwizacji na nośnikach zewnętrznych,
- Przeprowadzenie testów odtwarzania danych.

3.6 Integracja systemów

- Integracja komponentów infrastruktury IT i OT
- Integracja systemów bezpieczeństwa,
- Integracja rozwiązań open source,

3.7 Testy i uruchomienie produkcyjne

- Przeprowadzenie testów funkcjonalnych,
- Przeprowadzenie testów bezpieczeństwa,
- Przeprowadzenie testów wydajnościowych,
- Usunięcie wykrytych nieprawidłowości,
- Uruchomienie środowiska produkcyjnego.

3.8 Dokumentacja i przekazanie

- Opracowanie dokumentacji powdrożeniowej,
- Przekazanie konfiguracji i dostępu,
- Opracowanie procedur eksploatacyjnych,
- Przeprowadzenie szkolenia dla Administratorów Zamawiającego.

Wymagania dotyczące realizacji zamówienia

- Realizacja prac zgodnie z uzgodnionym harmonogramem,
- Minimalizacja wpływu prac na bieżące funkcjonowanie Zamawiającego,
- Zapewnienie wysokiej jakości wdrożenia,
- Stosowanie dobrych praktyk branżowych
- Zapewnienie udziału wykwalifikowanego personelu

Odbiór prac

- Odbiór realizowany na podstawie protokołu odbioru,
- Potwierdzenie poprawności działania wszystkich elementów infrastruktury,
- Weryfikacja kompletności dokumentacji,
- Przeprowadzenie testów akceptacyjnych.

7. Urządzenia brzegowe UTM z wbudowanymi kontrolerami WiFi wraz z niezbędnymi licencjami

Wymagania Ogólne

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

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

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje 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 umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 4 portami Gigabit Ethernet RJ-45.
 - Ponadto system realizujący funkcje firewall jest wyposażony w dwa interfejsy radiowe WiFi pracujące w standardach 802.11 a/b/g/n/ac/ax. Jeżeli takich interfejsów nie posiada, koniecznym jest zastosowanie urządzenia Access Point pracującego w w.w. standardach radiowych wraz z systemem centralnego zarządzania siecią WiFi (kontrolerem).
2. System Firewall posiada wbudowany port konsoli szeregowej.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. 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:

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

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. 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.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

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

- VMware NSX.
- Kubernetes.

Połączenia VPN

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

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje 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 umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w 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 chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

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

7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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).

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta **do dnia 31.12.2026**, 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.

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.

Wymagania dotyczące kwalifikacji personelu Wykonawcy

Wykonawca realizujący przedmiot zamówienia zobowiązany jest dysponować personelem posiadającym odpowiednią wiedzę, doświadczenie i kwalifikacje w zakresie projektowania, wdrażania, konfiguracji, administracji oraz utrzymania oferowanych rozwiązań bezpieczeństwa teleinformatycznego.

Subskrypcje i licencje:

1. **Kontrolę aplikacji (Application Control)** – identyfikację i kontrolę aplikacji oraz możliwość definiowania polityk dostępu na podstawie rozpoznanych aplikacji i kategorii aplikacji.
2. **System zapobiegania włamaniom (IPS – Intrusion Prevention System)** – wykrywanie i blokowanie prób wykorzystania podatności, ataków sieciowych oraz znanych zagrożeń na podstawie aktualizowanych sygnatur IPS.
3. **Ochronę antywirusową (Antivirus)** – wykrywanie i blokowanie złośliwego oprogramowania, wirusów, trojanów, ransomware oraz innych zagrożeń, z wykorzystaniem aktualizowanych baz sygnatur.
W ramach subskrypcji wymagane jest uwzględnienie sygnatur umożliwiających ochronę urządzeń mobilnych, co najmniej dla systemu operacyjnego Android.
4. **Analizę typu Sandbox w chmurze (Cloud Sandbox)** – możliwość przekazywania podejrzanych plików do analizy w środowisku izolowanym, w celu wykrywania nieznanych i zaawansowanych zagrożeń, w tym zagrożeń typu zero-day.
5. **Ochronę antyspamową (Anti-Spam)** – wykrywanie i blokowanie wiadomości zawierających spam, phishing oraz inne niepożądane lub potencjalnie niebezpieczne treści.
6. **Filtrowanie treści internetowych (Web Filtering)** – kontrolę dostępu do zasobów internetowych na podstawie kategorii stron, reputacji oraz klasyfikacji treści, wraz z dostępem do aktualizowanej bazy kategorii i reputacji stron internetowych.
7. **Bazy reputacyjne adresów IP i domen** – dostęp do aktualizowanych baz reputacyjnych umożliwiających identyfikację i blokowanie komunikacji z adresami IP oraz domenami powiązanymi ze złośliwą aktywnością, w tym między innymi z malware, botnetami, phishingiem i innymi zagrożeniami.
8. **Aktualizacje baz sygnatur i baz reputacyjnych** – zapewnienie bieżących aktualizacji baz wykorzystywanych przez wymienione mechanizmy bezpieczeństwa przez cały okres obowiązywania subskrypcji.

Okres obowiązywania licencji/subskrypcji: do dnia 31.12.2026.

8. Urządzenia brzegowe UTM wraz z niezbędnymi licencjami

Wymagania ogólne

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

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

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje 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 umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Zasilanie:

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

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołami SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

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

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołami minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).
 - Obsługę protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

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

Ochrona przed atakami

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

Kontrola aplikacji

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

7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

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

Testy wydajnościowe oraz funkcjonalne

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

Serwisy i licencje

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

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na **do dnia 31.12.2026.**

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta **do dnia 31.12.2026**, 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.

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.

Sposób spełnienia wymagania

Zamawiający dopuszcza, aby wymagane kompetencje były spełnione łącznie przez zespół osób skierowanych do realizacji zamówienia. Nie wymaga się, aby jedna osoba posiadała wszystkie wskazane certyfikaty.

Jedna osoba może jednocześnie potwierdzać spełnienie wymagań w więcej niż jednym obszarze. Certyfikaty powinny być aktualne na dzień wymagany dokumentacją postępowania, o ile dany program certyfikacyjny przewiduje okres ich ważności.

Na żądanie Zamawiającego Wykonawca przedstawi dokumenty umożliwiające weryfikację ważności i autentyczności wskazanych certyfikatów.

9. System do monitorowania infrastruktury i inwentaryzacji aktywów IT

Wymagania ogólne dla systemu zarządzania procesami, usługami i końcówkami

Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.

Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.

Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.

Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.

Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.

Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.

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.

Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.

Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).

Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przełączenia użytkownika konsoli systemu).

Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.

Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019

Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.

Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.

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.

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).

Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.

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).

Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.

Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).

Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.

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.

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.

Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.

Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.

Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.

Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.

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).

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.

Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.

Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.

Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.

Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.

Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.

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.

Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.

Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.

Oprogramowanie musi umożliwiać analizę sprzętową:

- płyty głównej w zakresie model, producent, nr. seryjny,
- CPU w zakresie nazwy, modelu, producenta, częstotliwości,
- HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
- RAM w zakresie wielkości pamięci,
- karty sieciowej w zakresie model, adres IP, adres MAC,
- karty graficznej w zakresie model.

Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.

Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.

Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.

Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.

Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.

Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.

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).

Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB.

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).

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

Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.

Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.

Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).

Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.

Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.

Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.

Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.

Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.

Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.

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

Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania.

Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).

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.

Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.

Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

CMDB

Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI).

Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe.

Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI.

Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny.

Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI.

Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji.
Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej.
Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji.
Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami.
Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)..
Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji.
Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów.
Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej.
Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji.

Zarządzanie zasobami oraz użytkownikami

Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiający powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
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.
Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu.
Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF.

Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków.

Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji.

Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu.

Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu.

Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu..

Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu.

Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego.

Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu.

Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami..

Oprogramowanie musi umożliwiać seryjne dodawanie zasobów.

Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów.

Oprogramowanie musi udostępniać kreator raportów dla zasobów.

Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu.

Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu .

Oprogramowanie musi umożliwiać ewidencję magazynów.

Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych.

Oprogramowanie musi umożliwiać ewidencję produktów magazynowych.

Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo).

Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM.

Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn.

Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu.

Oprogramowanie musi umożliwiać zwrot zasobów na magazyn.

Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM.

Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie.

Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca).

Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji.

Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników.

Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji.

Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników.

Oprogramowanie musi umożliwiać zarządzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami.

Zdalny pulpit, zdalne zarządzanie komputerem

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).

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.

Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).

Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.

Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.

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).

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.

Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.

Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.

Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.

Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.

Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe.

Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL.

Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows.

Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN.

Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połączenie konsoli ze wskazanym serwerem aplikacji.

Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

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.

Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.

Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.

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.

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 (polisą) odtworzeniem brakujących danych w przypadku wykrycia niespójności.

Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.

Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polisę wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).

Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).

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.

Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.

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.

Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.

Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:

1. 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)..
2. 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).
3. 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.
4. 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.
5. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.

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.)

Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji..

Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika.

Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera).

Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie).

Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej).

Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell).

Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.

Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).

Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.

Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.

Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów).

Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.

Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage

Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.

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.

Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USB Storage.

Oprogramowanie musi umożliwiać włączenie trybu Read Only dla klasy USB Storage.

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

Monitoring stanowisk komputerowych

Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.

Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.

Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).

Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach.

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).

Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.

Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.

Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).

Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.

Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania.

Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.

Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).

Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP.

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.

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.

Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

ServiceDesk - Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:

- Zarządzanie problemem
- Zarządzanie incydem
- Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
- Zarządzanie umowami serwisowymi
- Definicje poziomów SLA (reakcja, naprawa, reklamacja)

Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.

Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.

Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).

Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.

Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.

Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.

Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.

Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.

Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.

Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.

Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.

Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.

Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.

Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenie szablonów zadań.

Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.

Oprogramowanie musi umożliwiać przysyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.

Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.

Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.

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.

Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.

Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).

Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).

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.

Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.

Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.

Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.

Oprogramowanie musi umożliwiać przysyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.

Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji

mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.

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).

Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).

Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc).

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:

- Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
- Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
- Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
- Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
- Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
- Zamykanie zgłoszenia po upływie czasu reklamacji.
- Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
- Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
- Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
- Systemowe potwierdzanie realizacji zgłoszenia.
- Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.

Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.

Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.

Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.

Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika.

Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia.

Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń).

Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem.

Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB.

Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku).

Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia.

Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia.

Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja).

Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu.

Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą.

Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności.

Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu.

Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.

Oprogramowanie musi umożliwiać definiowanie obiegu za pomocą graficznego/blokowego kreatora.

Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.

Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.

Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.

Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.

Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.

Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.

Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

ServiceDesk – Zarządzanie wnioskami

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

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

ServiceDesk – Zarządzanie rezerwacjami

Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.

Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.

Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej - kalendarza.

Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Monitoring sieci LAN

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.

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.

Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.

Oprogramowanie musi umożliwiać z zdaną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.

Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.

Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.

Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.

Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Zarządzanie dokumentami

Oprogramowanie musi umożliwiać centralną ewidencję dokumentów.

Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu.

Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów).

Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów.

Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników.

Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym.

Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących.

Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany.

System wewnętrznego komunikatora dla użytkowników

Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.

Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2025 lub PostgreSQL.

Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.

Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami.

Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.

Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.

Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).

Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.

Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).

Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.

Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.

Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).

Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami.

Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania formalne

Dostarczone licencje na oprogramowanie muszą być bezterminowe.

Dostarczone licencje na oprogramowanie muszą być dostarczone z supportem producenta do dnia 31/12/2026.

W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp).

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.

Zamawiający wymaga, aby producent oferowanego oprogramowania przedstawił potwierdzenie (certyfikat), że oprogramowanie wytwarzane jest zgodnie z normą ISO27001.

Wymagania dotyczące zgodności z najlepszymi praktykami ITSM:

Zamawiający wymaga, aby oferowane oprogramowanie w zakresie:

- Zarządzanie incydentami (*Incident Management*),
- Zarządzanie problemami (*Problem Management*),
- Zarządzanie bazą wiedzy (*Knowledge Management*),
- Zarządzanie zasobami (*Asset Management*).

posiadało aktualny certyfikat zgodności z najlepszymi praktykami IT Service Management, wydany przez niezależną organizację certyfikującą.

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.

Zamawiający wymaga, aby Wykonawca dołączył do oferty oświadczenie producenta, które potwierdzi, że Wykonawca posiada odpowiednie kompetencje do wdrożenia proponowanego rozwiązania, a także że serwis będzie realizowany zarówno przez producenta, jak i przez Wykonawcę.

Ilość użytkowników: **80 szt.**

Wersja licencji: **wieczysta**

Wsparcie techniczne: **do dnia 31/12/2026**

Wdrożenie oprogramowania

Przedmiotem usługi jest instalacja i konfiguracja oprogramowania służącego do centralnego monitorowania oraz automatycznej inwentaryzacji infrastruktury informatycznej Zamawiającego.

W ramach realizacji usługi Wykonawca zapewni co najmniej:

- instalację i konfigurację systemu monitorowania i inwentaryzacji w środowisku Zamawiającego;
- konfigurację automatycznego wykrywania urządzeń pracujących w sieci LAN;
- inwentaryzację stacji roboczych, serwerów, urządzeń sieciowych oraz innych urządzeń posiadających interfejs sieciowy;
- gromadzenie informacji o sprzęcie, w szczególności: producencie, modelu, numerze seryjnym, procesorze, pamięci RAM, przestrzeni dyskowej, interfejsach sieciowych i adresacji IP;
- gromadzenie informacji o zainstalowanych systemach operacyjnych i oprogramowaniu;
- monitorowanie dostępności i podstawowych parametrów pracy urządzeń, serwerów oraz usług sieciowych;
- monitorowanie wykorzystania zasobów, w szczególności procesora, pamięci operacyjnej, przestrzeni dyskowej i interfejsów sieciowych;
- obsługę monitorowania urządzeń z wykorzystaniem standardowych protokołów i mechanizmów, w szczególności SNMP, ICMP, WMI/WinRM lub rozwiązań równoważnych;
- możliwość definiowania progów ostrzegawczych i krytycznych oraz generowania alertów w przypadku awarii, przekroczenia określonych wartości lub niedostępności urządzenia bądź usługi;
- możliwość wysyłania powiadomień o zdarzeniach co najmniej za pośrednictwem poczty elektronicznej;
- prowadzenie historii zdarzeń i zmian parametrów monitorowanych urządzeń;
- prezentację stanu infrastruktury za pomocą centralnego panelu administracyjnego;
- generowanie raportów dotyczących sprzętu, oprogramowania, dostępności urządzeń oraz wykrytych zdarzeń;
- możliwość eksportu raportów i danych do powszechnie stosowanych formatów;
- konfigurację kont użytkowników oraz odpowiednich uprawnień administracyjnych;
- konfigurację mechanizmu wykonywania kopii zapasowej konfiguracji i danych systemu;
- przeprowadzenie wstępnej inwentaryzacji infrastruktury Zamawiającego i dodanie wskazanych urządzeń do systemu monitorowania;
- konfigurację podstawowych reguł monitorowania, progów alarmowych oraz powiadomień;

- przekazanie Zamawiającemu dokumentacji powdrożeniowej obejmującej co najmniej opis konfiguracji, sposób wykonywania kopii zapasowej oraz podstawowe zasady administracji systemem;
- przeprowadzenie instruktażu dla administratora Zamawiającego w zakresie bieżącej obsługi wdrożonego rozwiązania.

System powinien umożliwiać dalszą rozbudowę zakresu monitorowanej infrastruktury bez konieczności wymiany wdrożonego rozwiązania.

Wykonawca zapewni wszystkie licencje niezbędne do prawidłowego działania systemu w zakresie określonym w dostawie systemu.

Wdrożenie należy wykonać w sposób zapewniający, że system monitorowania nie będzie powodował istotnego obciążenia monitorowanych urządzeń ani zakłóceń w funkcjonowaniu infrastruktury informatycznej Zamawiającego.

10. Szafa RACK na serwery

Szafa serwerowa RACK 19", stojąca, wysokość 42U, szerokość zewnętrzna 600 mm, głębokość zewnętrzna 1000 mm, wyposażona w panel LCD z wentylatorami oraz termostatem.:

- numerowane pionowe szyny montażowe
- przepusty kablowe w górnym i dolnym panelu,
- nośność szafy min. do 1000 kg
- 2 dedykowane półki w standardzie montażowym 19 cali o głębokościach roboczych od 650 mm do 780 mm, mocowane czteropunktowo
- 3 listwy zasilające poziome 19" (1U/2U): montowane bezpośrednio do pionowych szyn RACK, wyposażone w minimum 9 gniazd
- panel LCD z min. 2 wentylatorami

rodzaj szafy	wolnostojąca (serwerowa)
wysokość robocza	42U
szerokość montażowa	19"
minimalne wymiary zew. [mm]	600x1000
kolor	czarny
drzwi przednie	1-skrzydłowe - szkło hartowane lub perforowane
drzwi tylne	1-skrzydłowe - stal pełna lub perforowane
maksymalne obciążanie	Min. do 1000kg
Maksymalny kąt otwarcia drzwi przednich	min. 180°
Termostat	Tak
Panel LCD Tak	Tak
Klasa szczelności	IP20
Grubość drzwi przednich	min. 4 mm
Grubość górnego i dolnego panelu	min. 1,5 mm
Grubość bocznego panelu	min. 1 mm
Grubość szyn montażowych	min. 2 mm
Szczegóły uziemienia	Drzwi przednie, Drzwi tylne, Rama
Akcesoria w zestawie	Kółka z hamulcem, Kabel uziemiający, Nóżki, Pionowy organizator kabli, Panel wentylacyjny, Śruby, Termostat, Zamek przedni, Zamek tylny, Zamki boczne

11. Testy bezpieczeństwa sieci oraz serwisów www

W ramach usługi Wykonawca przeprowadzi testy bezpieczeństwa infrastruktury sieciowej Zamawiającego, którego celem będzie identyfikacja podatności, błędnych konfiguracji oraz potencjalnych wektorów ataku mogących wpływać na bezpieczeństwo infrastruktury IT Zamawiającego. Zakres usługi obejmuje w szczególności:

Przygotowanie i określenie zakresu testów

Wykonawca, w uzgodnieniu z Zamawiającym:

- określi zakres testowanej infrastruktury;
- zidentyfikuje adresację IP, urządzenia sieciowe, serwery, stacje robocze oraz inne zasoby objęte analizą;
- określi zakres testów wewnętrznych i/lub zewnętrznych;
- przygotuje harmonogram przeprowadzenia testów;
- określi zasady prowadzenia testów w sposób minimalizujący ryzyko zakłócenia pracy środowiska produkcyjnego.

Inwentaryzacja i identyfikacja zasobów

Wykonawca przeprowadzi identyfikację zasobów dostępnych w badanym środowisku, obejmującą w szczególności:

- urządzenia sieciowe;
- serwery;
- stacje robocze;
- systemy operacyjne;
- usługi sieciowe;
- aplikacje i komponenty infrastruktury;
- otwarte porty i dostępne usługi;
- zasoby dostępne z sieci wewnętrznej i zewnętrznej, w zakresie objętym testami.

Wyniki identyfikacji zostaną wykorzystane do dalszej analizy poziomu ekspozycji i ryzyka.

Skanowanie i identyfikacja podatności

Wykonawca przeprowadzi skanowanie bezpieczeństwa wskazanych zasobów w celu identyfikacji:

- znanych podatności bezpieczeństwa;
- nieaktualnego oprogramowania i komponentów;
- nieaktualnych systemów operacyjnych;
- błędów konfiguracji;
- niebezpiecznych lub niepotrzebnie dostępnych usług;
- otwartych portów i usług zwiększających powierzchnię ataku;
- potencjalnie niebezpiecznych ustawień zabezpieczeń;
- innych czynników mogących zwiększać ryzyko naruszenia bezpieczeństwa.

Analiza powierzchni ataku

Wykonawca przeprowadzi analizę ekspozycji infrastruktury Zamawiającego, obejmującą:

- identyfikację zasobów dostępnych z sieci;
- analizę potencjalnych punktów wejścia dla atakującego;
- identyfikację zależności pomiędzy zasobami;
- określenie potencjalnych ścieżek ataku;
- wskazanie zasobów o najwyższym poziomie ekspozycji;
- określenie potencjalnego wpływu wykrytych podatności na bezpieczeństwo środowiska.

Ocena i priorytetyzacja ryzyka

Wykonawca dokona analizy wykrytych podatności i nieprawidłowości oraz przypisze im poziom ryzyka, uwzględniając w szczególności:

- poziom krytyczności podatności;
- możliwość wykorzystania podatności;
- dostępność zasobu dla potencjalnego atakującego;
- znaczenie podatnego zasobu dla infrastruktury Zamawiającego;
- potencjalne skutki wykorzystania podatności;
- możliwość występowania zależności pomiędzy poszczególnymi podatnościami.

Wykonawca przygotuje priorytetyzację działań naprawczych, ze szczególnym uwzględnieniem podatności krytycznych i wysokiego ryzyka.

Analiza wyników testów

Wykonawca przeanalizuje wyniki przeprowadzonych testów i przygotuje zestawienie wykrytych problemów bezpieczeństwa, obejmujące co najmniej:

- identyfikację podatnego zasobu;
- opis wykrytej podatności lub nieprawidłowości;
- poziom ryzyka;
- potencjalne skutki wykorzystania podatności;
- rekomendowany sposób usunięcia lub ograniczenia ryzyka;
- priorytet wykonania działań naprawczych.

Raport z przeprowadzonych testów

Po zakończeniu testów Wykonawca przekaze Zamawiającemu raport z przeprowadzonych testów bezpieczeństwa, zawierający co najmniej:

- zakres i metodykę przeprowadzonych testów;
- opis badanego środowiska;
- wykaz zidentyfikowanych zasobów;
- wykaz wykrytych podatności i nieprawidłowości;
- klasyfikację podatności według poziomu ryzyka;
- opis potencjalnych skutków wykrytych problemów;
- wskazanie najważniejszych obszarów wymagających działań naprawczych;
- rekomendacje dotyczące usunięcia lub ograniczenia zidentyfikowanych zagrożeń;
- podsumowanie poziomu ekspozycji i bezpieczeństwa badanego środowiska.

Raport powinien zawierać zarówno część techniczną, przeznaczoną dla administratorów i osób technicznych, jak również podsumowanie zarządcze przedstawiające najważniejsze ryzyka i rekomendowane działania.

Omówienie wyników i rekomendacji

Wykonawca przeprowadzi z przedstawicielami Zamawiającego spotkanie podsumowujące, podczas którego:

- omówi wyniki przeprowadzonych testów;
- przedstawi najistotniejsze wykryte podatności;
- omówi najważniejsze ryzyka dla infrastruktury Zamawiającego;
- przedstawi rekomendowane działania naprawcze;
- wskaże priorytety usuwania wykrytych problemów.

Weryfikacja działań naprawczych

W przypadku usunięcia przez Zamawiającego wskazanych podatności lub nieprawidłowości Wykonawca, w zakresie uzgodnionym z Zamawiającym, przeprowadzi ponowną weryfikację

wybranych elementów środowiska w celu potwierdzenia skuteczności podjętych działań naprawczych

Przedmiotem usługi ma być kompleksowy Audyt Bezpieczeństwa zasobów teleinformatycznych Zamawiającego. Prace mają na celu wykrycie podatności na ataki z perspektywy zewnętrznego agresora oraz ocenę skuteczności wdrożonych mechanizmów obronnych.

Audyt ma zostać przeprowadzony zgodnie z najlepszymi praktykami rynkowymi i międzynarodowym standardami:

1. Testy zostaną przeprowadzone bez przekazywania Wykonawcy dokumentacji technicznej, haseł czy schematów sieci. Wykonawca powinien operować wyłącznie na informacjach publicznie dostępnych oraz pozyskanych w procesie rekonesansu, co w pełni symuluje działania realnego cyberprzestępcy.
2. Testy bezpieczeństwa (szczególnie w obszarze aplikacji i usług webowych) będą realizowane w oparciu o metodologię (Application Security Verification Standard), co gwarantuje sprawdzenie systemów pod kątem najczęstszych i najgroźniejszych wektorów ataków (np. SQL Injection, XSS, Broken Access Control).
3. Szczegółowy Zakres Czynności Testowych:
 - a) Rekonesans i OSINT: Pozyskanie informacji o infrastrukturze z otwartych źródeł oraz identyfikacja publicznych adresów IP i usług.
 - b) Testy penetracyjne infrastruktury zewnętrznej: Próby przełamania zabezpieczeń styku sieci z Internetem, analiza konfiguracji Firewall/VPN etc.
 - c) Wykrywanie podatności: Użycie profesjonalnych narzędzi do identyfikacji luk w oprogramowaniu serwerowym i sieciowym oraz praca testerów bezpieczeństwa.
 - d) Weryfikacja odporności na błędy logiczne: Próby obejścia mechanizmów autoryzacji i uwierzytelniania.
4. Raportowanie, Rekomendacje i Akredytacja

Po zakończeniu testów Zamawiający otrzyma minimum:

- a) Szczegółowy Raport Techniczny: Zawierający opis podatności, dowody (zrzuty ekranu, logi), ocenę ryzyka oraz konkretne wytyczne naprawcze.
- b) Akredytacja Bezpieczeństwa: Pozytywne zakończenie audytu (lub pomyślna weryfikacja napraw w ramach re-testu) zostanie potwierdzone wystawieniem przez Wykonawcę Certyfikatu/Akredytacji Bezpieczeństwa, poświadczającego, że infrastruktura została sprawdzona pod kątem zgodności ze standardami rynkowymi.

Dla usługi testów bezpieczeństwa infrastruktury sieciowej:

Podmiot realizujący usługę powinien posiadać wdrożone i certyfikowane systemy zarządzania zgodne z normami ISO/IEC 27001:2022 oraz ISO 9001:2015 lub normami równoważnymi, w zakresie adekwatnym do przedmiotu świadczonych usług.

Wykonawca wykaże, że dysponuje personelem posiadającym wiedzę i kwalifikacje w zakresie przeprowadzania testów bezpieczeństwa i testów penetracyjnych infrastruktury teleinformatycznej, potwierdzone odpowiednimi certyfikatami branżowymi, np. OSCP, OSEP, OSCE3, GPEN, GXPN, CEH lub certyfikatami równoważnymi.

Za certyfikat równoważny uznaje się certyfikat potwierdzający praktyczne kompetencje w zakresie identyfikacji podatności, rekonesansu, testów penetracyjnych infrastruktury sieciowej i systemowej, analizy podatności oraz opracowywania rekomendacji dotyczących usunięcia wykrytych nieprawidłowości.

12. Licencje wieczyste na system operacyjny dla serwerów

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Wbudowany asystent aktualizacji obejmujący możliwość upgrade z trzech ostatnich wersji systemu.
9. Narzędzie wiersza poleceń, które umożliwia użytkownikom monitorowanie i rozwiązywanie problemów z wydajnością systemu w czasie rzeczywistym, pozwalające dynamicznie instrumentować zarówno jądro, jak i kod w przestrzeni użytkownika bez konieczności modyfikowania samego kodu.
10. Wbudowana możliwość zakładania kont w systemie:
 - a. Microsoft Entra ID
 - b. Microsoft account
 - c. Work or school account.
11. Rozbudowane schematy Active Directory obejmujące sch89.ldf, sch90.ldf i sch91.ldf.
12. Poziom funkcjonalności domeny i lasu dostosowany rozmiar strony bazy danych 32k, odwzorowywany na wartość DomainLevel 10 i ForestLevel 10 dla instalacji nienadzorowanych.
13. Wystąpienia kontrolerów domeny i usług LDS w usłudze AD zezwalają protokołowi LDAP na dodawanie, wyszukiwanie i modyfikowanie operacji obejmujących atrybuty poufne tylko wtedy, gdy połączenie jest szyfrowane.
14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
17. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
18. Możliwość wykorzystania standardu http/2.

19. Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
20. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
21. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
22. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
23. Mechanizmy logowania w oparciu o:
 - a. Login i hasło,
 - b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
24. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
25. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
27. Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM).
28. Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0
29. Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu” kryptowalut.
30. Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe..
31. Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS.
32. Dostępność usługi Server Message Block (SMB) z szyfrowaniem AES-256 (AES-256-GCM and AES-256-CCM), automatycznie wykorzystywanych przy połączeniach z urządzeniami wspierającymi te metody.
33. Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego.
34. Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure.
35. Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny.
36. Wsparcie migracji zasobów na dyskach do Azure.
37. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
38. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
39. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
40. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

- b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- c. Zdalna dystrybucja oprogramowania na stacje robocze.
- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
- e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - i. Dystrybucję certyfikatów poprzez http
 - ii. Konsolidację CA dla wielu lasów domeny,
 - iii. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
 - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f. Szyfrowanie plików i folderów.
- g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
- i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- j. Serwis udostępniania stron WWW.
- k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- l. Wsparcie dla algorytmów Suite B (RFC 4869),
- m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
- o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- q. Mechanizmy wirtualizacji mające wsparcie dla:
 - i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - iii. Obsługi 4-KB sektorów dysków
 - iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

- v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
 - vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
41. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
 42. Wsparcie dla rozwiązania Kubernetes.
 43. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
 44. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
 45. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
 46. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 47. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
 48. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
 49. Mechanizm konfiguracji połączenia VPN do platformy Azure.
 50. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
 51. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
 52. Zorganizowany system szkoleń i materiały edukacyjne w języku polski.

Oświadczenie Wykonawcy.

Oświadczam, że składając ofertę świadom jestem jej złożenia i zapewniam, że wykonam zamówienie zgodnie z oczekiwaniami Zamawiającego.

Składając ofertę oświadczam, że spełniam warunki udziału w postępowaniu.

Oświadczam, że wykonam zamówienie zgodnie z wymaganiami zawartymi w niniejszym Opisie Przedmiotu Zamówienia.

....., dnia