1. **Zakres przedmiotu zamówienia:**

Przedmiotem zamawiania jest:

1. Dostawa i wdrożenie, w tym instalacja i konfiguracja systemu teleinformatycznego:
2. **klasy SIEM**, który agreguje dane zdarzeń z urządzeń zabezpieczających, sieci, systemów operacyjnych oraz aplikacji, a następnie analizuje te dane w celu zapewnienia zarządzania bezpieczeństwem IT;
3. **typu HelpDesk**, który odpowiada m.in. za przyjmowanie zgłoszeń od użytkowników oraz kontrolę ich rozwiązania;
4. zapewnienie 5-letniego pakietu gwarancyjnego i licencyjnego dla ww. systemów teleinformatycznych;
5. przeszkolenie pracowników Zamawiającego w zakresie eksploatacji i obsługi systemu;
6. zapewnienie usług wsparcia Wykonawcy w wymiarze maksymalnie do 300 godzin dla ww. systemów teleinformatycznych.
7. **Ogólne wymagania Systemu klasy SIEM:**
8. musi wspierać przeglądarki m.in.: Edge, Chrome, Firefox i inne;
9. nie dopuszcza się rozwiązań typu open surce;
10. musi być zapewniony dostęp do systemu dla użytkownika za pośrednictwem konsoli webowej oraz z aplikacji mobilnej;
11. musi być w całości dostępny interfejs systemu oraz konfiguracji z poziomu przeglądarki internetowej bez potrzeby instalacji tzw. grubego klienta;
12. musi być wielojęzyczny interfejs, w tym w języku polskim;
13. musi być zapewniona personalizacja:
14. musi mieć możliwość dostosowania strony logowania oraz edytowania plików HTML i CSS,
15. użytkownicy muszą mieć możliwość personalizowania swoich profili, w tym dodawać zdjęcia i dodatkowe opisy;
16. musi pozwalać na tworzenie dedykowanych widoków dla każdego użytkownika. Widoki muszą być filtrowane i sortowane według atrybutów zgłoszeń, takich jak status, priorytet, użytkownik, czy czas rozwiązania;
17. musi posiadać pływające menu, które jest widoczne niezależnie od położenia ekranu, co umożliwia szybki dostęp do najważniejszych funkcji;
18. musi pozwalać na personalizację portalu metodą drag & drop, umożliwiając użytkownikom dostosowanie rozmieszczenia elementów portalu oraz wstawianie treści HTML lub wideo;
19. musi mieć możliwość filtrowania i wyboru prezentowanych danych według dowolnych atrybutów zgłoszeń, takich jak numer zgłoszenia, kategoria, czas rozwiązania;
20. musi mieć możliwość tworzenia przez użytkowników własnych, dedykowanych pulpitów do monitorowania kluczowych wskaźników wydajności oraz sygnalizacji zagrożeń, takich jak przepustowość, zużycie procesora i inne.
21. musi mieć widoki dostosowane do potrzeb użytkownika, tak aby była możliwość definiowania przez użytkowników własnych filtrów logów, dodawanie raportów w postaci widżetów oraz dostosowywania wyglądu pulpitu;
22. musi umożliwiać dostęp użytkownikom do predefiniowanych raportów oraz tworzenia raportów niestandardowych na temat użytkowników, grup, polityk bezpieczeństwa, uprawnień do folderów oraz innych aspektów zarządzania Active Directory.
23. **Zakres wymagań funkcjonalnych Systemu klasy SIEM:**
24. **Log Management System (LMS) - audyt i monitoring**
25. System musi umożliwiać audyt zdarzeń zarówno w czasie rzeczywistym, jak i w ustawianych interwałach czasowych;
26. System musi wspierać automatyczne wykrywanie hostów;
27. System musi umożliwić w zakresie infrastruktury stacji robaczych i serwerów audyt oraz monitoring:
28. bez instalacji dodatkowych klientów na serwerach,
29. urządzeń USB dla Serwerów Windows i systemu Windows (zmiany na plikach lub folderach, odczyt, zmiana, kopiowanie plików),
30. zmian na udostępnieniach sieciowych (zmiany nazw plików i folderów, tworzenie, usuwanie, przenoszenie, zmiany uprawnień),
31. wszystkich certyfikatów systemów,
32. zmian na serwerach członkowskich,
33. serwera plików,
34. stanu usługi DNS, zmiany strefy, zmiany rekordów, zmiany konfiguracji i inne zmiany powiązane z DNS’ami,
35. ilość komputerów - wyświetlać ilość nieaktywnych komputerów, w ciągu 30 dni,
36. w następujących obszarach RAID:
* zasoby fizyczne,
* kontrolery,
* zasoby logiczne,
* luny,
* partycje,
* grupy raid,
* grupy dysków wirtualnych,
* woluminy,
* grupy woluminów.
1. musi umożliwiać w zakresie infrastruktury sieciowej audyt oraz monitoring:
2. aktywny - urządzeń sieciowych oraz pasywny - przez odbieranie i procesowanie pułapek SNMP,
3. wydajności SNMP podczas wykrywania serwerów, które zostały wykryte bez monitorów domyślnych, z wykorzystaniem odpowiednich poświadczeń SNMP,
4. wydajności dla procesu aktualizacji poświadczeń SNMP v1/v2, aby zapewnić szybsze i bardziej efektywne zarządzanie urządzeniami sieciowymi,
5. zdarzeń dotyczących sieci WiFi (nawiązanie i rozłączenie połączenia WiFi),
6. połączeń LDAP SSL, bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów,
7. czasu rozpoczęcia i zakończenia replikacji usługi AD - śledzenie zmian replikacji, awarie i inne,
8. urządzeń sieciowych oraz kontrolerów sieci bezprzewodowej (WLC),
9. urządzeń sieciowych:
* Środowisk z systemem operacyjnym Microsoft Windows przez poświadczenia WMI,
* Środowisk Linux/Unix przez wykorzystanie poświadczeń CLI (dostęp przez SSH/Telnet),
* Pozostałych urządzeń sieciowych obsługujących protokół SNMP v1/2/3.
1. VPN (Site-to-Site) dla połączeń obsługiwanych przez następujących dostawców: Cisco, WatchGuard i Fortinet,
2. segmentów sieci w infrastrukturze IT,
3. danych typu ARP z urządzeń Cisco,
4. serwera DHCP od Fortinet,
5. firewalle producentów: Cisco, Fortinet, PfSense, Huawei,
6. Wireless LAN Controller (WLC) dla urządzeń różnych dostawców.
7. musi umożliwiać w zakresie oprogramowania systemowego oraz serwerowego audyt oraz monitoring:
8. hostów środowisk wirtualnych VMware i HyperV,
9. zdarzeń sysmon,
10. kontrolerów domeny Active Directory, w tym:
* Procesów LSASS,
* Procesów NTFRS,
* Statystyk bazy danych,
* Uwierzytelnienia Kerberos na sekundę,
* Replikacji usługi Active Directory,
* Nowych połączeń LDAP,
* Uwierzytelnień NTLM na sekundę.
1. zmian w zasadach grupowych (tworzenie, usuwanie, lista zmodyfikowanych GPO, historia GPO),
2. zmian uprawnień (dostęp do domeny, zmiany OU, kontenery, GPO, użytkownicy, grupy, komputery, DNS),
3. zmian w zasadach grupowych (tworzenie, usuwanie, lista zmodyfikowanych GPO, historia GPO),
4. serwerów MS SQL i Exchange,
5. komponentów IT z wykorzystaniem własnych skryptów napisanych w Powershell, Linux shell script, VBScript, Perl lub Python oraz przypisywanie wartości brzegowych oraz profili powiadomień dla wyników tych skryptów,
6. Integralności plików.
7. musi umożliwiać w zakresie usług chmurowych audyt oraz monitoring:
8. serwera plików od Azure (Azure File Share),
9. nadanych ról w Azure Active Directory (przypisanie, odłączenie członka od roli),
10. zmian grup w Azure Active Directory (utworzenie, usunięcie, aktualizacja grup, dodanie/usunięcie członków),
11. poprawnych i niepoprawnych logowań użytkowników w Azure Active Directory,
12. usług w chmurze w celu klasyfikowania usług internetowych na podstawie adresów IP,
13. musi umożliwiać w zakresie zarządzenia i uprawnień użytkownikami audyt oraz monitoring:
14. podstawowych danych nt. Active Directory, w tym:
* wyświetlać ilość wszystkich użytkowników;
* wyświetlać ilość nieaktywnych użytkowników, w ciągu 30 dni;
* wyświetlać ilość zablokowanych użytkowników;
* wyświetlać ilość wyłączonych użytkowników;
* wyświetlać ilość użytkowników z wygaśniętym hasłem;
* wyświetlać ilość użytkowników, którzy nigdy się nie zalogowali;
* wyświetlać ilość użytkowników, którzy zalogowali się w ciągu ostatnich 30 dni,
1. sesji użytkownika,
2. aktywności logowań użytkowników (logowania i wylogowania) do stacjach roboczych,
3. zmian kont na stacjach roboczych (tworzenie, usuwanie, dezaktywacja, historia),
4. zmian na kontach użytkowników w Active Directory (tworzenie, usuwanie, dezaktywacja kont, modyfikacja haseł, spis zablokowanych użytkowników, historia użytkowników),
5. zmian na kontach użytkowników Azure Active Directory (utworzenie, usunięcie, aktualizacja, aktywacja, dezaktywacja, zmiana hasła, reset hasła),
6. poprawnych i niepoprawnych logowań użytkowników w Azure Active Directory
7. nadanych ról w Azure Active Directory (przypisanie, odłączenie członka od roli),
8. zmian grup w Azure Active Directory (utworzenie, usunięcie, aktualizacja grup, dodanie/usunięcie członków),
9. zmian w zasadach grupowych (tworzenie, usuwanie, lista zmodyfikowanych GPO, historia GPO),
10. zmian uprawnień (dostęp do domeny, zmiany OU, kontenery, GPO, użytkownicy, grupy, komputery, DNS),
11. dostępu do plików i zmiany uprawnień w systemach pamięci masowej Huawei OceanStor,
12. zmian w uprawnieniach użytkowników oraz dostęp do historii zmian w tych uprawnieniach.
13. **Security Information Management (SIM) - analiza i generowanie raportów:**
14. System musi umożliwiać generowanie raportów dotyczących zarządzanych zasobów, systemów operacyjnych i zainstalowanych aplikacji,
15. System musi wspierać analizę logów dotyczących aktywności użytkowników na monitorowanych urządzeniach,
16. System musi umożliwiać dywersyfikację uprawnień przynajmniej na dwa poziomy – administrator i użytkownik tylko do odczytu,
17. System musi pozwalać generować raporty automatycznie na podstawie ustalonego harmonogramu w formatach takich jak PDF i CSV.
18. System musi umożliwiać w zakresie infrastruktury stacji robaczych i serwerów analizę i wygenerować:
19. raporty dotyczące urządzeń (logowanie, zarządzanie regułami zapory, zdarzenia systemowe, ważność certyfikatów),
20. raporty dotyczące serwerów i kontrolerów domen,
21. raporty zablokowanych kont, czas ostatniego logowania / wylogowania, rodzaj systemu operacyjnego, itd.,
22. raporty dostępu do poszczególnych folderów,
23. raporty użytkowników,
24. raporty bezpieczeństwa,
25. raporty logowania,
26. raporty z usługi Exchange,
27. raporty haseł,
28. raporty GPO,
29. raporty stacji roboczych,
30. raporty grup,
31. raporty polis,
32. raporty jednostek organizacyjnych,
33. raporty udziałów NTFS,
34. raporty uprawnień i dostępu do katalogów,
35. raporty Office365: raporty użytkowników; raporty grup; raporty kontaktów; raporty licencji; raporty skrzynek pocztowych; raporty OWA;
36. raporty dynamiczne grup dystrybucyjnych,
37. raporty użytkowników nieobecnych, usuniętych z Active Directory,
38. raporty dotyczących bibliotek taśmowych różnych producentów, obejmujących przynajmniej następujące obszary:
* zasoby fizyczne,
* sterowniki taśm,
* porty taśm,
* sterowniki dostępu,
* porty bibliotek scsi,
* zasoby logiczne,
* partycje,
* napędy.
1. System musi dokonać w zakresie infrastruktury sieciowej analizy i wygenerować:
2. raporty dotyczące interfejsów LAN-WAN,
3. raporty ruchu zawierających szczegóły dotyczące źródła, miejsca docelowego oraz konwersacji, bazujące na adresach MAC, z integracją DHCP,
4. analizę wysycenia pasma w technologii NetFlow,
5. raporty dotyczące urządzeń (logowanie, zarządzanie regułami zapory, zdarzenia systemowe),
6. raporty typu „prognoza”, które pozwalają na oszacowanie przyszłego pasma,
7. raporty ruchu dla systemów autonomicznych (AS) i dla Cisco Medianet,
8. raporty według ustalonego harmonogramu czasowego i przesyłanie ich za pomocą poczty elektronicznej w formacie PDF, XLS.
9. System musi dokonać w zakresie oprogramowania systemowego oraz serwerowego analizy i wygenerować:
10. raporty dotyczące urządzeń (logowanie, zarządzanie regułami zapory, zdarzenia systemowe, ważność certyfikatów),
11. raporty integralności plików.
12. System musi dokonać w zakresie usług chmurowych analizy i wygenerować:
13. raporty usług chmurowych (SaaS, IaaS, PaaS),
14. raporty dla zdarzeń z Azure AD.
15. System musi dokonać w zakresie zarządzenia i uprawnień użytkownikami analizy i umożliwić wygenerować:
16. raporty dotyczące aktywności użytkowników oraz przypisanych im uprawnień,
17. raporty użytkowników stacji roboczych (tworzenie, usuwanie, dezaktywacja kont, modyfikacja haseł, historia użytkowników),
18. raporty Active Directory (nieudane próby logowania, poprawne logowanie użytkowników, zmiany na kontach użytkowników),
19. raport dotyczące uprawnień i polityk dostępu,
20. raport zmian uprawnień w celu dostarczenia informacji o wartościach uprawnień przed i po,
21. raport z audytów uprawnień, pokazujących zmiany w dostępie do zasobów i funkcji,
22. raport aktywności użytkowników w zakresie zarządzania dostępem oraz zmianami wprowadzanymi przez użytkowników.
23. **Security Event Management (SEM) - wizualizacja danych, korelacje zdarzeń oraz alarmowanie:**
	1. System musi umożliwiać wykonanie automatycznych działań po wykryciu nowego urządzenia (np. przydzielenie do określonej grupy, dodanie określonych parametrów monitorowania, dodanie określonych profili powiadomień w oparciu o schemat nazwy DNS,
	2. System musi umożliwiać audyt wszystkich historycznych działań wykonywanych na urządzeniach, wraz z informacjami o czasie ich wykonania oraz osobie odpowiedzialnej,
	3. System musi umożliwiać audyt wszystkich historycznych działań wykonywanych na urządzeniach, wraz z informacjami o czasie ich wykonania oraz osobie odpowiedzialnej,
	4. System musi umożliwiać automatyczne uruchamianie skryptów naprawczych i weryfikacyjnych w przypadku przekroczenia wartości brzegowych dla zdefiniowanych monitorów,
	5. System musi posiadać opcję masowego rozwiązywania żądań przepływu pracy, niezależnie od statusu zgłoszenia,
	6. System musi pozwalać na konfigurację następujących działań w momencie wystąpienia alarmu:
24. wysłanie powiadomienia email,
25. wysłanie powiadomienia sms,
26. wykonanie komendy w wierszu poleceń,
27. uruchomienie programu/skryptu,
28. wysłanie wiadomości syslog,
29. wygenerowanie pułapki snmp,
30. zarejestrowanie zgłoszenia,
31. rejestrację ticketu w osobnym systemie wsparcia użytkownika integrującym się z omawianym systemem monitorowania.
	1. System musi pozwalać na planowanie i eksportowanie zintegrowanych raportów w formacie pliku XLS,
	2. System musi umożliwiać włączenie uwierzytelniania dwuskładnikowego,
	3. System musi obsługiwać bazy danych PostgreSQL i MSSQL,
	4. System musi być zoptymalizowany do pracy na platformach Windows, zapewniające pełną funkcjonalność i stabilność,
	5. System musi wykonywać wszystkie operacje związane z przechowywaniem i zarządzaniem danymi na jednej, centralnej bazie danych, co zapewnia spójność, efektywność oraz łatwość zarządzania informacjami,
	6. System musi automatycznie przełączać się na zapasową instancję, w przypadku awarii głównej instancji, zapewniając ciągłość działania bez przestojów,
	7. System musi obsługiwać „ElasticSearch”, umożliwiając zaawansowane wyszukiwanie i analizę danych w czasie rzeczywistym,
	8. System musi wymuszać autoryzowany dostęp,
	9. System musi wspierać kompleksowe monitorowanie i audytowanie wszystkich działań związanych z bezpieczeństwem, w tym logowania, zmian w konfiguracji i dostępie,
	10. System musi umożliwiać generowanie raportów dotyczących zagrożeń, zapewniając szczegółową analizę potencjalnych ryzyka i incydentów bezpieczeństwa.
	11. System w zakresie infrastruktury stacji robaczych i serwerów:
32. musi pozwolić na dynamicznie ustawiać wartości progowe dla kluczowych monitorów, takich jak wydajność procesora, wykorzystanie pamięci i czas odpowiedzi. Dzięki temu użytkownicy mogą lepiej optymalizować wydajność otrzymywanych alertów, dostosowując je do zmieniających się warunków i potrzeb operacyjnych,
33. musi umożliwiać monitorowanie oraz dostarczanie informacji w postaci raportów dotyczących przynajmniej następujących obszarów RAID:
* zasoby fizyczne,
* kontrolery,
* zasoby logiczne,
* luny,
* partycje,
* grupy raid,
* grupy dysków wirtualnych,
* woluminy,
* grupy woluminów.
1. musi zapewniać wbudowane narzędzia umożliwiające wykonywanie kluczowych operacji na bazie danych, takich jak tworzenie backupów, odtwarzanie bazy danych oraz zmiana używanej bazy danych,
2. musi umożliwiać realizację wszystkich operacji związanych z autoryzacją i dostępem do zasobów w domenie za pomocą jednego konta,
3. musi umożliwiać różne poziomy dostępu w celu delegacji zadań do pracowników bez konieczności dystrybucji uprawnień administratora, z możliwością ograniczenia zadań do poszczególnych jednostek organizacyjnych oraz domen. W szczególności: reset hasła użytkownika, odblokowanie konta użytkownika, dodawanie i usuwanie członków grup, przenoszenie użytkowników do różnych jednostek organizacyjnych w ramach domeny, dodawanie i usuwanie stacji roboczych w domenie, tworzenie kont użytkowników, a także tworzenie, usuwanie i modyfikacja atrybutów kont użytkowników,
4. musi umożliwiać zarządzanie stacjami roboczymi w Active Directory, w tym: zbiorcze dodawanie i usuwanie stacji roboczych z grup; zbiorcze przypisywanie ogólnych atrybutów, takich jak opis i lokalizacja, do stacji roboczych; zbiorcze blokowanie i odblokowywanie stacji roboczych; zbiorcze przenoszenie stacji roboczych pomiędzy jednostkami organizacyjnymi (OU) w domenie,
5. musi umożliwiać zarządzanie udziałami plików na serwerach plików, a w szczególności: zbiorcze modyfikowanie uprawnień NTFS do plików/folderów; zbiorcze usuwanie uprawnień NTFS do plików/folderów,
6. musi umożliwiać wykonywanie kopii zapasowej obiektów z Active Directory,
7. musi umożliwiać logowanie lokalne oraz z wykorzystaniem poświadczeń domenowych Active Directory,
8. musi umożliwiać przeszukiwanie zdarzeń archiwalnych dla platformy Azure AD,
9. musi umożliwiać konfigurację Azure Active Directory (Azure AD) bez konieczności konfiguracji lokalnej domeny Active Directory,
	1. System w zakresie infrastruktury sieciowej:
10. musi wspierać zarówno IPv4, jak i IPv6,
11. musi posiadać wbudowaną funkcję zarządzania adresacją IP,
12. musi posiadać moduł analizy logów zapór sieciowych,
13. musi pozwolić na monitorowanie ruch sieciowego za pomocą technologii NetFlow, aby w czasie rzeczywistym identyfikować wysycenie pasma. Powinien zapewniać możliwość analizy danych przepływu, umożliwiając administratorom szybkie wykrywanie przeciążeń oraz diagnozowanie przyczyn problemów, takich jak nadmierne wykorzystanie przez określone aplikacje, ataki DDoS czy nieefektywne trasy. Ponadto, system powinien wspierać działania prewencyjne, takie jak automatyczna optymalizacja ruchu, aby zapobiegać obniżeniu jakości usług sieciowych i utrzymać płynność działania sieci,
14. musi posiadać funkcjonalność automatycznego generowania map sieci z wykorzystaniem mechanizmów CDP, LLDP, IPROUTE, FDP oraz ARP,
15. musi umożliwiać definiowanie grup adresów IP, co pozwala na filtrowanie raportów, określanie sumarycznego ruchu w zależności od użytego interfejsu, portu, protokołu lub adresu IP, a także na analizę parametrów RTT (Round-Trip Time) w sieciach WAN,
16. musi wspierać i analizuje przepływ danych w formacie IPv6,
17. musi umożliwiać zarządzanie konfiguracją urządzeń sieciowych, w tym:
* składowanie konfiguracji,
* automatyczne tworzenie kopii zapasowych,
* wersjonowanie kopii zapasowych,
* porównywanie różnych wersji konfiguracji,
* tworzenie kopii zapasowych zgodnie z harmonogramem,
* dystrybucję konfiguracji i fragmentów konfiguracji na wybranej grupie urządzeń oraz grupowanie ich z odpowiednimi vendorami,
* weryfikację konfiguracji z politykami zgodności,
1. musi umożliwiać tworzenie kopii zapasowych "out-of-the-box" dla urządzeń następujących producentów:
* Cisco,
* Dell,
* Fortinet,
* Huawei,
1. musi umożliwiać skanowanie przełączników sieciowych w celu weryfikacji dostępności i zajętości portów oraz identyfikacji urządzeń podłączonych do tych portów,
2. musi wyświetlać przyczynę niepowodzenia skanowania zakresu IP przy użyciu DHCP,
3. musi umożliwiać analizę tuneli VPN i serwerów proxy w czasie rzeczywistym,
4. musi pozwolić na zarządzanie regułami firewalla dla urządzeń: FortiGate,
5. musi umożliwiać zarządzanie politykami firewalla za pomocą API dla urządzeń FortiGate,
6. musi umożliwiać zarządzanie adresacją IP oraz portami przełączników sieciowych,
7. musi umożliwiać analizę logów zapór sieciowych,
8. musi pozwalać na analizę ruchu dla interfejsów fizycznych i logicznych na przełącznikach lub routerach,
9. musi umożliwić definiowanie alarmów, w tym według adresów IP, które są uruchamiane po przekroczeniu zdefiniowanych progów i generują wiadomości e-mail lub pułapki SNMP,
10. musi umożliwić integrację z narzędziem typu APM, co pozwala na dokładniejsze monitorowanie ruchu sieciowego pochodzącego z serwerów, aplikacji oraz usług.
11. musi umożliwić przechwytywanie pakietów internetowych na urządzeniach, które nie obsługują technologii flow, a następnie konwertowanie ich na odpowiedni pakiet flow i wysyłanie do systemu.
12. musi umożliwić przechowywanie niezagregowanych danych o ruchu sieciowym (2 lata).
	1. System w zakresie oprogramowania systemowego oraz serwerowego:
13. musi zapisywać nieudane próby logowania na serwery Radius oraz historia logowań,
14. musi zapisywać sumaryczne dane dotyczące nieudanych prób logowania w domenie na podstawie przyczyny błędu logowania.
	1. System w zakresie usług chmurowych:
15. musi zarządzać Office365:
* zarządzenie użytkownikami;
* zarządzenie grupami;
* zarządzanie kontaktami;
* zarządzanie licencjami;
* zarządzanie skrzynkami mailowymi;
* zarządzanie udostępnionymi skrzynkami mailowymi;
* zarządzanie kalendarzem,
1. musi zarządzać kanałami i politykami w Microsoft Teams,
2. musi wykonywać kopię oraz przywracanie platformy Azure Active Directory - użytkownicy, grupy, urządzeń, aplikacji, ról oraz domen.
	1. System w zakresie zarządzenia i uprawnień użytkownikami:
3. musi analizować zachowania przy użyciu uczenia maszynowego oraz analizy statystycznej (nietypowa aktywność użytkownika, nietypowa aktywność na serwerze, nietypowa ilość prób logowań, nietypowe godziny logowań, nietypowe działania na plikach),
4. musi monitorować użytkowników połączeni z dużą ilością zasobów,
5. musi monitorować konta o dużej aktywności,
6. musi monitorować konta o nadmiernej aktywności,
7. musi monitorować konta z wysokim % niepowodzeń logowania,
8. musi monitorować ostatnią aktywność użytkownika,
9. musi monitorować uśpione konta administratorów,
10. musi monitorować uprawnienia wykorzystane przez użytkowników,
11. musi monitorować pierwsze użycie przydzielonego uprawnienia,
12. musi monitorować konta oparte na zdalnym logowaniu,
13. musi monitorować zmiany uprawnień (dostęp do domeny, zmiany OU, kontenery, GPO, użytkownicy,
14. musi monitorować nieudane próby logowani do środowiska domenowego,
15. musi monitorować poprawne logowania użytkowników wraz z pełną historią logowania,
16. musi monitorować nieudane prób logowania na serwery Radius oraz historia logowań,
17. musi monitorować zmiany nazw użytkowników/komputerów/grup,
18. musi wykorzystywać algorytmy uczenia maszynowego do oceny ryzyka związanego z aktywnością użytkowników,
19. musi posiadać mechanizm oceny ryzyka tożsamości w AD,
20. musi posiadać mechanizm ocena ryzyka tożsamości dla Microsoft 365,
21. musi posiadać API do wykonywania następujących czynności w wybranej domenie:
* tworzenie OU;
* tworzenie użytkownika, wg. predefiniowanych w systemie szablonów;
* restartowanie hasła użytkownika;
* odblokować/zablokować użytkownika;
* usunięcie użytkownika;
* wyszukiwanie konkretnego użytkownika w AD;
* wymuszenia synchronizacji z AD, przed podaniem wyników wyszukiwania;
* posortowania wyników według wybranej kolumny;
* posortowania wyników rosnąco lub malejąco;
* ustawić datę, w której wygaśnie konto użytkownika;
* przenoszenie użytkowników pomiędzy wybranymi jednostkami organizacyjnymi (OU); wyszukiwanie odpowiednich OU oraz ich usuwanie;
* możliwość wyszukiwania, włączania, wyłączania, usuwania, dodawania lub usuwania z grup, przenoszenie do wybranych jednostek organizacyjnych dla komputerów,
1. musi posiadać mechanizm zarządzania użytkownikami Active Directory, a w szczególności:
* tworzenie i modyfikację grup Active Directory;
* tworzenie kont użytkowników dla wielu użytkowników, w tym unikanie tworzenia duplikatów, poprzez wykorzystywanie dodatkowych elementów w loginie;
* modyfikacja atrybutów dla wielu użytkowników;
* reset haseł i odblokowanie kont dla wielu kont użytkowników;
* zmiana wyświetlanej nazwy użytkownika;
* tworzenie skrzynek mailowych systemu Exchange;
* udostępnianie / blokowanie / usuwanie nieaktywnych kont w Active Directory;
* przenoszenie użytkowników między jednostkami organizacyjnymi (OU)
1. musi tworzyć nowych użytkowników w Active Directory, a w szczególności:
* tworzenie użytkowników przez definiowanie wszystkich atrybutów z uwzględnieniem usług Exchange, Terminal, Lync, Office365; dodawanie użytkowników przez kopiowanie właściwości innego użytkownika;
* import właściwości użytkownika z plików CSV, gdzie jedynym obowiązkowym atrybutem jest nazwa użytkownika;
* tworzenie i wykorzystanie szablonów z wspólnymi atrybutami;
* tworzenie użytkowników w istniejącym kontenerze lub tworzenie nowej jednostki organizacyjnej (OU) i dodanie do niej użytkowników,
1. musi pozwolić na zbiorcze modyfikowanie kont użytkowników w Active Directory, a wszczególności:
* reset haseł dla wielu kont; ustawianie haseł nigdy nie wygasających;
* ustawianie haseł, których użytkownik nie może zmienić;
* ustawianie haseł, które użytkownik ma obowiązek zmienić przy następnym logowaniu;
* usuwanie i blokowanie użytkowników, jeżeli ich hasło wygasło,
* musi pozwolić na zarządzanie użytkownikami i konfiguracji systemu:
* modyfikacja formatów nazwy, nazwy wyświetlanej, nazwy logowania i nazwy kont SAM (Security Account Manager);
* udostępnianie / blokowanie użytkowników, odblokowywanie użytkowników, definiowanie czasu wygaśnięcia kont;
* definiowanie katalogów głównych (Home Folder), profile i ścieżek skryptów dla użytkowników;
* aktualizacja członkostwa grup i list dystrybucyjnych;
* przenoszenie użytkowników do innych kontenerów;
* tworzenie skrzynek na serwerze Exchange dla użytkowników;
* definiowanie wielkości wiadomości przychodzących i wychodzących oraz innych ograniczeń;
* ograniczenie limitów adresatów i adresów przekierowania dla użytkowników;
* modyfikację limitów składowania poczty i retencji usuniętych obiektów;
* udostępnianie / blokowanie dostępu mobilnego do programu Outlook (również w wersji Web), protokołów IMAP4 i POP3;
* modyfikację katalogu głównego usług terminalowych i ścieżek profilowych dla użytkowników;
* modyfikację programów startowych dla użytkowników logujących się z usług terminalowych;
* modyfikację czasu trwania sesji, limitu aktywnych sesji, limitu bezczynnych sesji, itd.;
* udostępnianie / blokowanie parametrów zdalnej kontroli;
* zarządzanie kontami użytkowników nieaktywnych i zablokowanych;
* wyszukiwanie kont użytkowników lub stacji roboczych nie logowanych przez zdefiniowaną ilość dni;
* wyszukiwanie wygasłych i niewykorzystywanych kont Active Directory;
* lokalizację nieaktywnych kont użytkowników lub stacji roboczych i blokowanie, usuwanie, przenoszenie lub aktywację tych kont,
1. musi pozwolić na konfigurację uprawnień GPO (edycja, modyfikowanie zabezpieczeń, odczyt lub usuwanie) dla żądanych użytkowników, grup i komputerów,
2. musi system wspiera różnorodne poziomy dostępu, od administratora po użytkownika z ograniczonym dostępem, oraz pozwala na przypisanie uprawnień według określonych ról.
3. **Ogólne wymagania Systemu typu HELPDESK (logowanie, raportowanie oraz wykrywania zagrożeń):**
4. musi mieć wsparcie dla Azure SQL,
5. nie dopuszcza się rozwiązań typu open surce;
6. musi mieć możliwość integracji z dowolną skrzynką pocztową działająca na protokole m.in.: POP, POPS, IMAP, IMAPS, SMTP, SMTPS, Exchange Online,
7. musi mieć możliwość logowania bez potrzeby ponownego używania poświadczeń do aplikacji (SAML SSO),
8. musi mieć darmową aplikację mobilną na systemy Android i iOS,
9. musi mieć moduł ankietowania,
10. musi mieć możliwość integracji z rozwiązaniem Teams firmy Microsoft,
11. musi mieć dwuskładnikowe logowanie,
12. musi mieć możliwość integracji z kalendarzem firmy Microsoft,
13. musi mieć możliwość integracji z Active Directory lub LDAP, wsparcie dla logowanie single Sign On bez konieczności instalowania dodatkowych aplikacji,
14. musi mieć dostęp do interfejsu systemu oraz konfiguracji w całości dostępny z poziomu przeglądarki internetowej bez potrzeby instalacji tzw. grubego klienta,
15. musi mieć interfejs systemu dostępny w języku polskim,
16. musi mieć rozwiązanie pozwalające na rejestrowanie nieobecności i wyznaczanie zastępstw dla techników. Automatyczne przekierowanie zgłoszeń do wskazanego technika zapasowego/zastępczego (bazując na dacie zarejestrowania zgłoszenia bądź dacie rozwiązania zgłoszenia) lub wyłączenie umowy SLA dla zgłoszenia,
17. musi mieć zarządzanie procesami, tworzenie harmonogramów dla zgłoszeń okresowych, automatyczne przydzielanie zadań do serwisantów,
18. musi mieć możliwość wstawianie plików graficznych oraz materiałów video w treści rozwiązania zgłoszenia,
19. musi spełnianie wymagań RODO poprzez możliwość oznaczania danych jako danych zawierających dane osobowe oraz automatycznej animizacji danych przy usunięciu użytkownika z aplikacji
20. musi mieć moduł AI do szkolenia w celu automatyzacji zadań pomocy technicznej,
21. musi mieć dwuskładnikowe uwierzytelnianie dla dostępu do panelu administracyjnego,
22. musi mieć możliwość natywnej integracji z systemami SCCM, z narzędziami Microsoft 365Atlassian Jira,
23. musi mieć możliwość rejestrowania aktywności i zleceń pracy związanych z poszczególnymi incydentami.
24. **Zakres wymagań funkcjonalnych dla Systemu typu HELPDESK:**
25. **Moduł HelpDesk:**
26. musi mieć moduł zarządzania procesami,
27. musi mieć możliwość przekazywania wiadomości od serwisanta, bezpośrednio na skrzynkę pocztową zgłaszającego,
28. musi umożliwiać użytkownikowi w trakcie rejestracji zgłoszenia na stronie www:
29. załączenie dowolnej ilości dowolnego formatu załączników;
30. system pozwala na wymuszenie na użytkowniku końcowym konieczność dodania załącznika do zgłoszenia,
31. musi mieć możliwość udostępniania do wglądu zgłoszenia pomiędzy serwisantami oraz zgłaszającymi, zgłoszenie może być udostępnione dla poszczególnych użytkowników lub w grupy w obrębie działów użytkowników,
32. musi mieć możliwość przeglądania przez użytkowników na stronie www statusu własnych zgłoszeń, dodawania komentarzy, podgląd i edycję danych użytkownika, przeglądania bazy wiedzy znanych problemów i ich rozwiązań,
33. musi mieć możliwość definiowania dodatkowych pól w formularzu incydentu,
34. musi mieć możliwość konfiguracji wyzwalania różnych akcji poprzez uruchomienie dedykowanego skryptu z możliwością wyzwalania akcji na systemie zintegrowanym z systemem helpdeskowym,
35. musi mieć centralne repozytorium incydentów, umożliwiające filtrowanie i sortowanie zapisanych zgłoszeń według co najmniej następujących kryteriów: status zgłoszenia, kategoria, użytkownik, czas rozwiązania, czas przyjęcia, przydzielona grupa wsparcia,
36. musi mieć centralne repozytorium incydentów, zapewniające definiowanie własnych filtrów umożliwiających sortowanie zapisanych zgłoszeń,
37. musi mieć możliwość tworzenia harmonogramów dla zgłoszeń okresowych, a w ramach realizacji takiego zgłoszenia automatyczne przydzielanie zadań do serwisantów.
38. **Moduł zgłoszeń:**
39. musi mieć możliwość wymuszania podawania komentarzy przy zmianie statusów zgłoszenia,
40. musi określić dla każdego zgłoszenia atrybuty takie jak: dane osoby zgłaszającej oraz priorytet realizacji,
41. musi mieć możliwość przeszukiwania zgłoszeń według co najmniej następujących atrybutów: numer zgłoszenia, użytkownik, tytuł, opis,
42. musi mieć spis zarejestrowanych zgłoszeń, w tym widok prezentujący listę zarejestrowanych zgłoszeń incydentów i zadań,
43. musi mieć możliwość wyboru i filtrowania danych dla każdego z widoku zgłoszeń i zadań, według wszystkich dostępnych atrybutów w zgłoszeniu i zadaniu,
44. musi mieć możliwość rejestracji zgłoszeń pochodzących z zewnętrznych narzędzi monitorujących, jednocześnie umożliwiając ich klasyfikację i na tej podstawie automatyczne przekazywanie do grup wsparcia,
45. musi mieć edycję zgłoszenia po jego zarejestrowaniu,
46. musi mieć możliwość klasyfikacji zgłoszeń, w co najmniej 3 poziomowej strukturze drzewiastej, struktura klasyfikacji musi być dowolnie edytowalna przez uprawnionych administratorów z poziomu interfejsu systemu,
47. musi mieć automatyczną eskalację zgłoszeń do grup wsparcia, na podstawie co najmniej następujących atrybutów: poziom, tytuł zgłoszenia, słowo kluczowe w tytule,
48. musi mieć możliwość przekierowania zgłoszeń do innych serwisantów lub grup wsparcia celem dalszej obsługi,
49. musi mieć możliwość tworzenia szablonów zgłoszeń z predefiniowanymi atrybutami i regułami przekazywania tychże zgłoszeń do zespołów wsparcia,
50. musi mieć możliwość definiowania na formularzach, pól niezbędnych do wypełnienia w trakcie rejestracji i zamknięcia zgłoszenia,
51. musi mieć możliwość definiowania i filtrowania szablonów zgłoszeń dedykowanych dla określonych grup użytkowników,
52. musi mieć możliwość przekazywania do akceptacji osób trzecich działań podejmowanych w ramach rozwiązania zgłoszenia, np. akceptacja realizacji zlecenia na usługę serwisową,
53. musi mieć możliwość automatycznego przypisywania osób wymaganych do akceptacji zgłoszenia w oparciu o sposób wypełnienia zgłoszenia, akceptacje mogą być oparte o dowolne atrybuty zgłaszającego oraz dane osoby zgłaszającej,
54. musi mieć możliwość przeglądania bazy wiedzy z poziomu incydentu i podłączania rozwiązania z bazy rozwiązań do rozwiązania w zgłoszeniu,
55. **Moduł powiadomienia**
56. musi mieć możliwość globalnego definiowania szablonów email do powiadamiania użytkowników o różnych zdarzeniach w systemie,
57. musi mieć możliwość przesyłania i prezentowania na stronie www powiadomień dla użytkowników i/lub serwisantów, przesyłania powiadomień do pojedynczych użytkowników lub grup użytkowników/serwisantów,
58. musi mieć możliwość przesyłania powiadomień do użytkowników o zdarzeniach zarejestrowanych przez system takich jak: przyjęcie zgłoszenia, aktualizacja zgłoszenia, rozwiązanie zgłoszenia, zamknięcie zgłoszenia.
59. **SLA**
60. musi mieć możliwość zdefiniowania umów SLA w oparciu o priorytet,
61. musi mieć możliwość implementacji warunków umów SLA, obliczania czasu rozwiązania incydentu.
62. **Moduł zarzadzanie wiedzą**
	1. musi mieć bazę wiedzy umożliwiającą rejestrację rozwiązań zawierających co najmniej następujące atrybuty, temat i opis rozwiązania, powiązane słowa kluczowe, klasyfikacja rozwiązania,
	2. musi mieć bazę wiedzy umożliwiającą przeszukiwanie danych po dowolnych atrybutach systemu,
	3. mus mieć możliwość udostępniania rozwiązań osobno dla użytkowników i osobno dla serwisantów,
	4. musi mieć możliwość rejestracji rozwiązań z poziomu incydentu,
	5. musi mieć możliwość dokonania akceptacji dodawanego do bazy wiedzy rozwiązania przez administratora bazy wiedzy,
	6. musi mieć możliwość zamieszczania i wyświetlania w treści rozwiązania plików graficznych oraz dołączania dowolnej ilość załączników,
	7. musi mieć możliwość ukrycia bazy wiedzy przed zgłaszającymi,
	8. bazy wiedzy musi posiadać API.
63. **Moduł raporty**
64. musi mieć możliwość prezentowania w postaci graficznej wskaźników wydajności pozwalających na monitorowanie statusu poszczególnych procesów, wskaźniki odświeżane o konfigurowalny interwał czasu;
65. musi mieć możliwość prezentowania użytkowników z wykorzystaniem imienia i nazwiska, a także dowolnie rozbudowanymi atrybutami – możliwość automatycznego wypełnienia stworzonych atrybutów z danych Active Directory,
66. musi mieć możliwość rejestracji czasu pracy nad zgłoszeniem,
67. musi mieć możliwość raportowania zarejestrowanych incydentów, problemów i zmian filtrowanych według kategorii, departamentu, statusu zgłoszenia, użytkownika,
68. musi mieć możliwość raportowania rozkładu incydentów w czasie według dowolnego atrybutu,
69. musi mieć możliwość raportowania czasu pracy użytkowników w ramach rozwiązywania zgłoszeń,
70. musi mieć możliwość automatycznego tworzenia raportów, zdefiniowanych według cyklicznego harmonogramu, a następnie przesyłanie tychże raportów za pomocą poczty elektronicznej do dowolnego użytkownika,
71. musi mieć dostęp do modułu raportowego tylko wybranym pracownikom,
72. musi mieć możliwość exportu utworzonych raportów do plików formatu HTML, PDF, XLS, XLSX, CSV, DOC, DOCX, XML,
73. **Moduł WIDOKI**
74. musi mieć możliwość edycji tablic wskaźników w oparciu o mechanizm przeciągania i upuszczania poszczególnych obiektów na tablicy wskaźników,
75. **Moduł zarządzanie zasobami**
76. musi mieć możliwość zbierania danych o konfiguracji sprzętu: skanowanie urządzeń Windows, macOS, Linux; skanowanie urządzeń z wykorzystaniem Telnet/SSH skanowanie urządzeń z wykorzystaniem SNMP V1, V2, V3,
77. musi mieć możliwość przypisania zasobu do użytkownika, działu, lokalizacji,
78. musi mieć możliwość wprowadzania zasobów skanowanych po kodzie kreskowym,
79. musi mieć możliwość generowania kodów kreskowych dla zasobów – definiowalny przez użytkownika formatu kodu kreskowego i jego wydruk,
80. musi mieć możliwość wykrywania zmian w konfiguracji i generowanie raportów porównawczych zmian w elementach konfiguracji,
81. musi mieć możliwość przeprowadzania automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu,
82. musi mieć możliwość zarządzania licencjami oprogramowania poprzez ich rejestrowanie w systemie, licencja posiada informacje co najmniej o typie licencji, dozwolonej ilości instalacji, kluczu licencji,
83. musi umożliwiać prezentację ilości licencji,
84. musi mieć wypożyczalnię sprzętu użytkownikom, która pozwala na:
	1. określenie zasobów możliwych do wypożyczenia;
	2. określenie maksymalnego czasu trwania wypożyczenia;
	3. określenie przyczyny wypożyczenia;
	4. weryfikowanie listy wypożyczonego sprzętu;
	5. powiadamianie użytkowników o konieczności zwrócenia wypożyczonego sprzętu,
85. grupowanie zasobów w sposób statyczny lub dynamiczny,
86. określenie statusu zasobu oraz dodawanie własnych statusów np: w magazynie, w naprawie, wydany itp.
87. **Moduł Katalog Usług**
88. tworzenie, edycja, usuwanie, kopiowanie formularzy wniosków o usługę,
89. konfiguracja przebiegu akceptacji dla wniosków o usługę,
90. konfiguracja do 5 etapów akceptacji,
91. dodanie więcej jak jednej osoby na każdym etapie akceptacji,
92. konfiguracja akceptacji, aby wymagana była zgoda wszystkich osób występujących w procesie akceptacji,
93. konfiguracja akceptacji, aby wymagana była zgoda tylko jednej osoby z osób występujących w procesie akceptacji,
94. konfiguracja dodatkowych sekcji w formularzu wniosku o usługę, które pozwalają na dodawanie zdjęć/obrazów oraz kosztów,
95. konfiguracji przebiegu akceptacji za pomocą API.
96. **Moduł zarządzanie problemami**
97. musi mieć możliwość konfiguracji formularza do zgłaszania problemu,
98. musi mieć możliwość konfiguracji dodatkowych pól w formularzu problemu takich jak: pole tekstowe jednowierszowe; pole tekstowe wielowierszowe; pole typu „lista”; pole numeryczne; pole typu „kalendarz”,
99. musi mieć możliwość konfiguracji zadań w formularzu „problemu”,
100. musi mieć możliwość tworzenia, edycji, usuwania, kopiowania formularzy „problemu”,
101. musi mieć możliwość określania wpływu, głównej przyczyny oraz symptomów „problemu”,
102. musi mieć określenie rozwiązania tymczasowego oraz docelowego „problemu”,
103. musi mieć możliwość powiązania „problemu” z „incydentami” oraz ze „zmianą”,
104. musi mieć możliwość kopiowania rozwiązania „problemu” do wszystkich powiązanych „incydentów”,
105. musi mieć możliwość zamknięcia wszystkich powiązanych „incydentów” podczas zamykania „problemu”; możliwość konfiguracji pól wymaganych do zamknięcia „problemu”,
106. musi mieć możliwość wysyłania powiadomień do użytkowników dla wybranych działań w zarejestrowanym „problemie”.
107. **Moduł zarządzanie „zmianami”**
108. musi mieć możliwość konfiguracji „zmiany” np.: typ zmiany, etap zmiany, status zmiany,
109. musi mieć możliwość konfiguracji, tworzenia, edycji, usuwania, kopiowania formularzy „zmiany” oraz możliwość konfiguracji pól w formularzu „zmiany” np. pole tekstowe jednowierszowe, pole tekstowe wielowierszowe, pole typu „lista”,
110. musi mieć możliwość powiązania przebiegu „zmiany” z formularzem „zmiany”,
111. musi mieć możliwość dodawania zadań oraz notatek do zarejestrowanej „zmiany”,
112. musi mieć możliwość powiązania „zmiany” z „problemem”, „projektem” oraz „wydaniem”,
113. musi mieć możliwość prezentacji harmonogramu przyszłych „zmian” w postaci graficznej, w rozbiciu na różne typy „zmian”,
114. musi mieć możliwość wysyłania powiadomień do użytkowników dla wybranych działań w zarejestrowanej „zmianie”.
115. **Moduł zarządzanie Wydaniami**
116. musi mieć możliwość konfiguracji, tworzenia, edycji, usuwania, kopiowania formularzy Wydania,
117. musi mieć możliwość konfiguracji dodatkowych pól w formularzu Wydania np. pole tekstowe jednowierszowe, pole tekstowe wielowierszowe, pole typu Lista, pole wielokrotnego wyboru, pole typu checkbox,
118. musi mieć możliwość konfiguracji: etap Wydania, status Wydania, rola Wydania,
119. musi mieć możliwość powiązania przebiegu Wydania z formularzem Wydania,
120. musi mieć możliwość dodawania zadań oraz notatek do zarejestrowanego Wydania,
121. musi mieć możliwość powiązania Wydania ze Zmianą oraz Projektem,
122. musi mieć powiązanie Wydania z Zasobem,
123. musi mieć możliwość wysyłania powiadomień do użytkowników dla wybranych działań w zarejestrowanym Wydaniu.
124. **Baza danych konfiguracji**
125. musi mieć możliwość dodawania, edycji, usuwania własnych typów elementów konfiguracji oraz przechowywanie danych o wszystkich jednostkach konfiguracji,
126. musi mieć możliwość dodawania, edycji, usuwania typów relacji między elementami konfiguracji,
127. musi mieć dynamiczne rozszerzanie schematu danych o dodatkowe atrybuty, w tym atrybuty dedykowane dla konkretnego typu elementu konfiguracji,
128. musi mieć możliwość przedstawiania w sposób graficzny wzajemnych relacji pomiędzy elementami konfiguracji;
129. musi mieć możliwość przechowywania relacji pomiędzy incydentami, problemami oraz zmianami, a elementami konfiguracji,
130. musi mieć możliwość ręcznego dodawania elementów konfiguracji oraz relacji pomiędzy nimi,
131. musi mieć możliwość importu elementów konfiguracji z pliku CSV oraz relacji pomiędzy nimi z pliku XLS;
132. musi mieć moduł wykrywania środowiska IT, pozwalający na wykrycie co najmniej konfiguracji komputerów, serwerów i oprogramowania; wykrywanie opiera się na: skanowanie agentowe; skanowanie telnet/SSH; skanowanie Vmware; skanowanie SNMP v1/v2/v3; integracja z SCCM;
133. musi mieć możliwość przechowywania informacji o poszczególnych elementach konfiguracji tak, aby możliwe było rejestrowanie i śledzenie historii posiadania elementu konfiguracji przez użytkowników, powiązanie z nim informacji o koszcie zakupu, innych kosztach eksploatacyjnych, warunkach umowy serwisowej, dostawcy,
134. musi mieć możliwość wyszukiwania elementów konfiguracji po dowolnych atrybutach, zarówno standardowych, jaki i dodanych przez użytkownika, w tym po kodach kreskowych,
135. musi mieć możliwość definiowania wartości początkowej elementu konfiguracji oraz mierzenie jego amortyzacji;
136. musi mieć możliwość powiązania poszczególnych elementów konfiguracji z danymi użytkownika (jego imieniem i nazwiskiem, nr telefonu, departamentem), departamentu, innymi elementami konfiguracji i katalogiem usług.
137. **Wdrożenie systemu**

Wykonawca zobowiązuje się do wdrożenia systemu zgodnie z poniższym opisem.

1. Analiza i projekt wdrożenia.
2. Analiza obecnej konfiguracji sieci, wykorzystywanych rozwiązań bezpieczeństwa, w tym integracja systemu klasy SIEM z istniejącą infrastrukturą sieciową, firewallami, serwerami, aplikacjami i innymi zasobami.
3. Analiza możliwości przeniesienia bieżących reguł i konfiguracji systemów do nowego systemu klasy SIEM oraz nowego systemu typu HelpDesk.
4. Analiza integracji Systemów z zasobami Zamawiającego, w tym:
5. Dystrybucja i konfiguracja klientów VPN użytkowników.
6. Integracja z Active Directory, Forti Analyzer, Forti EMS oraz innymi narzędziami używanymi przez Zamawiającego.
7. Integracja z systemami chmurowymi, takimi jak Azure.
8. Integracja systemów kontroli dostępu do sieci (NAC), systemów bezprzewodowych (WiFi) i innych powiązanych elementów sieci.
9. Propozycje i zalecenia dotyczące bieżącego wdrożenia oraz możliwości jego dalszej rozbudowy w przyszłości.
10. Wykonanie projektu wdrożenia przed konfiguracją systemu.
11. Zamawiający ma 5 dni roboczych na akceptację lub zgłoszenie uwag do projektu technicznego. Warunkiem rozpoczęcia wdrożenia jest zatwierdzenie projektu technicznego przez Zamawiającego.
12. Przeprowadzenie warsztatów dotyczących proponowanej architektury i konfiguracji systemu.
13. Instalacja i prace wdrożeniowe.
	1. Instalacja i podstawowa konfiguracja systemów SIEM i HelpDesk.
	2. Integracja systemów SIEM i HelpDesk z systemami wewnętrznymi, takimi jak Active Directory, Forti Analyzer, Intune.
	3. Konfiguracja systemów do monitorowania, zarządzania uprawnieniami, generowania raportów oraz zarządzania incydentami bezpieczeństwa.
	4. Optymalizacja konfiguracji systemu w oparciu o wymagania Zamawiającego, w tym definicja reguł korelacji zdarzeń i automatyzacja odpowiedzi na incydenty.
	5. Konfiguracja dostępu użytkowników i przypisanie odpowiednich poziomów uprawnień w systemach.
14. Testy usług.
15. Przeprowadzenie testów funkcjonalności, w tym testów wydajnościowych i bezpieczeństwa.
16. Przeprowadzenie testów akceptacyjnych, obejmujących wszystkie kluczowe funkcje systemów SIEM i HelpDesk.
17. Przeprowadzenie optymalizacji konfiguracji po wdrożeniu systemu w oparciu o wyniki testów.
18. Przygotowanie pełnej dokumentacji powdrożeniowej systemu, w tym konfiguracji, reguł monitorowania i zarządzania incydentami.
19. **5-letni pakiet gwarancyjny i licencyjny:**
20. Gwarancja systemu.
21. System klasy SIEM oraz system typu HelpDesk będą objęte 5-letnią gwarancją producenta oraz licencją na wszystkie funkcjonalności opisane w niniejszej dokumentacji, w tym na aktualizacje oprogramowania oraz wsparcie techniczne.
22. W przypadku wadliwego działania systemu lub jego niestabilności, gwarancja obejmuje naprawę systemu lub jego komponentów do końca następnego dnia roboczego od zgłoszenia problemu.
23. Warunki gwarancyjne.
24. Przez cały okres gwarancji Zamawiający będzie mieć dostęp do najnowszych wersji oprogramowania systemów klasy SIEM i HelpDesk, w tym do aktualizacji bezpieczeństwa, poprawek oraz nowych funkcjonalności, które zostaną udostępnione w ramach licencji.
25. Naprawy systemów będą realizowane przez producenta, wykonawcę lub inny podmiot upoważniony przez producenta do świadczenia takich usług.
26. Procedura napraw.
27. Naprawy będą wykonywane w siedzibie Zamawiającego, o ile Strony nie uzgodnią inaczej. W przypadkach, gdy naprawa na miejscu nie będzie możliwa, wykonawca zorganizuje transport systemu do serwisu, a po naprawie zwróci go do Zamawiającego na własny koszt.
28. W razie potrzeby naprawy poza siedzibą Zamawiającego, wykonawca zobowiązuje się do ponownej instalacji systemu w środowisku Zamawiającego po naprawie.
29. Zgłaszanie usterek.
30. Zgłoszenia serwisowe mogą być dokonywane w języku polskim, 24 godziny na dobę, przez wszystkie dni w tygodniu.
31. Pakiet gwarancyjny obejmuje naprawę, wymianę części, czy też całych elementów systemu na nowe, oryginalne części zgodnie z zaleceniami producenta.
32. Warunki obsługi gwarancyjnej.
33. Wszelkie usługi gwarancyjne, w tym naprawy, wymiany i aktualizacje systemu, będą realizowane w siedzibie Zamawiającego w dni robocze, w godzinach 8:00–16:00, o ile Strony nie uzgodnią inaczej.
34. Naprawy lub wymiany będą realizowane zgodnie z ustalonym harmonogramem, z możliwością wykonania pilnych napraw w krótszym czasie, jeśli będzie to wymagane.
35. Na czas naprawy Zamawiający otrzyma system zastępczy, który umożliwi nieprzerwane funkcjonowanie kluczowych procesów.
36. Wsparcie techniczne.
37. Wykonawca zapewni pełne wsparcie techniczne przez okres 5 lat, w tym:
38. Koordynowanie zgłoszeń gwarancyjnych.
39. Aktualizacje oprogramowania.
40. Pomoc techniczną w ramach zainstalowanych systemów SIEM i HelpDesk.
41. Wykonawca zobowiązuje się do monitorowania i zarządzania zgłoszeniami serwisowymi oraz do zapewnienia szybkiej reakcji na wszelkie problemy związane z działaniem systemów.
42. Gwarancja obejmuje również wsparcie w zakresie rekonfiguracji systemów oraz aktualizacji wynikających z ewolucji potrzeb Zamawiającego zmian technologicznych lub siedziby przez Zamawiającego.
43. Regularne przeglądy i audyty systemu będą przeprowadzane w uzgodnionych terminach, aby zapewnić optymalne działanie systemów i ich zgodność z obowiązującymi standardami bezpieczeństwa.
44. **Przeszkolenie pracowników Zamawiającego w zakresie eksploatacji i obsługi nowego systemu klasy SIEM i systemu typu HeplDesk**
	1. Przeszkolenie wdrożeniowe obejmuje pracowników Zamawiającego, maksymalnie 10 osób.
	2. Zakres przeszkolenia będzie obejmował administrację, eksploatację i obsługę Systemu.
	3. Przeszkolenia będą przeprowadzane w siedzibie Zamawiającego z możliwością uczestniczenia on-line przez pracowników Zamawiającego, poprzez wykorzystanie użytkowanej przez Zamawiającego aplikacji Microsoft Teams.
	4. Przeszkolenia będą prowadzone w ramach warsztatów.
	5. Przeszkolenia będą prowadzone w oparciu o dokumentację techniczną i eksploatacyjną Systemu.
	6. Każde przeszkolenie będzie trwało do wyczerpania materiału, ale nie dłużej niż 4 godziny dziennie. Jeżeli materiał przeszkolenia nie zostanie wyczerpany w jednym (4-godzinnym) przeszkoleniu, możliwe będzie dokończenie tego materiału w ramach kolejnego przeszkolenia z tego zakresu, przeszkolenie będzie trwało maksymalnie 2 dni robocze.
	7. W przypadku, gdyby ilość przeszkoleń okazała się niewystarczająca, Zamawiający może zamówić dodatkowy instruktaż w ramach puli roboczogodzin przeznaczonych na usługi wsparcia.
45. **Usługi wsparcia Wykonawcy**
46. Wykonawca zobowiązuje się do świadczenia usług wsparcia technicznego przez okres 4 lat od daty zawarcia umowy lub do wyczerpania puli godzin wsparcia, w zależności od tego, co nastąpi wcześniej.
47. Pula godzin wsparcia wynosi maksymalnie 350 godzin.
48. Wsparcie będzie realizowane w dni robocze, w godzinach 7:30–15:30, o ile Strony nie uzgodnią inaczej. W przypadkach wyjątkowych wsparcie może być świadczone w innych godzinach, o czym Zamawiający poinformuje Wykonawcę z wyprzedzeniem 5 dni roboczych.
49. Usługi wsparcia mogą być realizowane zdalnie lub w siedzibie Zamawiającego, jeśli realizacja zdalna okaże się niemożliwa lub nieefektywna.
50. Procedura wsparcia:
51. Zgłoszenie wsparcia:

Zamawiający zgłasza potrzebę wsparcia Wykonawcy wraz z opisem problemu.

1. Odpowiedź Wykonawcy:

Wykonawca w ciągu 2 dni roboczych od otrzymania zgłoszenia odpowie na zapytanie, ustalając szczegóły realizacji wsparcia.

1. Realizacja wsparcia:

Specjaliści Wykonawcy przystąpią do realizacji wsparcia w ciągu 2 dni roboczych od ustalenia szczegółów zlecenia.

1. Sytuacje awaryjne:

W sytuacjach nieprzewidzianych, wymagających natychmiastowej reakcji, wsparcie zostanie zrealizowane na zasadach specjalnych. Pierwsze dwie godziny takiego wsparcia będą liczone podwójnie (1 godzina odpowiada 2 godzinom z puli wsparcia).

1. Zakres wsparcia:

Wsparcie obejmuje między innymi:

1. Koordynowanie zgłoszeń gwarancyjnych:
2. Przygotowanie i przekazanie zgłoszenia do producenta/serwisu, monitorowanie statusu zgłoszenia oraz zapewnienie odpowiednich działań naprawczych.
3. Prace rekonfiguracyjne, diagnostyczne i projektowe:

Usługi te obejmują zmiany konfiguracji systemu, analizy wydajności oraz projektowanie nowych rozwiązań w oparciu o rozwój infrastruktury.

1. Opracowanie dokumentacji:

Przygotowanie pełnej dokumentacji technicznej dotyczącej zrealizowanych prac i działań w ramach wsparcia.

1. Aktualizacje systemu:

Przeprowadzanie niezbędnych aktualizacji oprogramowania SIEM i HelpDesk, w tym poprawki bezpieczeństwa i nowe funkcjonalności.

1. Przeszkolenia:

Przeprowadzanie przeszkoleń dla administratorów Zamawiającego w zakresie eksploatacji, konfiguracji oraz zarządzania systemami bezpieczeństwa (SIEM) oraz innymi powiązanymi elementami infrastruktury (VPN, WiFi, firewall).

1. Wstępna wycena pracochłonności:

Strony będą uzgadniały przed realizacją każdego zlecenia wstępny szacunek liczby godzin potrzebnych na realizację wsparcia. Dopuszczalna różnica między rzeczywistym czasem realizacji a wstępnym szacunkiem wynosi +/- 20%.