

OPIS PRZEDMIOTU ZAMÓWIENIA

I.	DOSTĘP DO PLATFORMY SZKOLENIOWEJ DLA PRACOWNIKÓW JST	2
II.	OPROGRAMOWANIE DO INWENTARYZACJI SPRZĘTU I OPROGRAMOWANIA	6

I. DOSTĘP DO PLATFORMY SZKOLENIOWEJ DLA PRACOWNIKÓW JST

Wykonawca zapewni dostęp do platformy szkoleniowej dla 185 użytkowników. Wykonawca zobowiązany jest przekazać zamawiającemu dostęp do platformy na okres 24 miesięcy.

1. WYMAGANIA MINIMALNE PLATFORMY SZKOLENIOWEJ:

Kompleksowa platforma *security awareness* dostarczająca organizacjom narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. Użytkownicy otrzymują dostęp do materiałów szkoleniowych oraz testów wiedzy. Menedżerowie grup oraz administratorzy zyskują wgląd w postęp nauki i poziom wiedzy w całej organizacji dla poszczególnych grup.

1.1. Platforma zawiera co najmniej:

- 1.1.1. Materiały szkoleniowe podzielone na 12 modułów w 65 lekcjach.
- 1.1.2. 17 testów wiedzy.
- 1.1.3. Statystyki i raporty dla użytkowników, grup i menadżerów.
- 1.1.4. Platforma powinna być stale rozwijana pod kątem funkcjonalnym jak i zwiększaniem zawartości szkoleniowej.

1.2. Architektura Platformy

- 1.2.1. Platforma musi być systemem chmurowym, który nie wymaga konserwacji przez Zamawiającego.

1.3. Cechy organizacji

- 1.3.1. Po zakupie subskrypcji, Zamawiający otrzymuje wyłączny dostęp do nowo utworzonej organizacji. Nazwa organizacji jest definiowana w trakcie procesu zakupowego. Wspólnie z Zamawiającym tworzone jest konto Administratora Głównego. Administratorem danych konta Administratora Głównego jest Producent rozwiązania.
- 1.3.2. W każdej organizacji istnieje jedno konto Administratora Głównego. Administrator Główny dodaje lub importuje konta pierwszych użytkowników do platformy. Administratorem danych użytkowników Organizacji jest Administrator Główny.
- 1.3.3. Administrator Główny może powierzyć zadanie zarządzania organizacją innym użytkownikom poprzez nadanie im roli Administratora.
- 1.3.4. Każda organizacja może mieć maksymalnie 5000 użytkowników oraz 1000 grup.

1.4. Część szkoleniowa

- 1.4.1. Platforma udostępnia swoim użytkownikom kurs z zakresu cyberbezpieczeństwa "Bezpieczna praca w Internecie", który składa się z min. 12 modułów, 65 lekcji i 17 testów sprawdzających nabytą przez kursantów wiedzę. Każdy moduł składa się z 4-7 lekcji w formie video oraz testu. Oprócz testów wewnątrz modułu, kurs zawiera również testy obejmujące swoim zakresem tematycznym przekrojowo więcej niż 1 moduł szkoleniowy.
- 1.4.2. Szkolenie powinno zostać przygotowane i odpowiednio ułożone przez ekspertów w dziedzinie cyberbezpieczeństwa, a informacje w nim zawarte są aktualne, istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera w pracy i nie tylko.

1.5. Minimalny zakres tematyczny:

- 1.5.1. socjotechniki,



- 1.5.2. bezpieczeństwo haseł,
- 1.5.3. bezpieczeństwo poczty e-mail i ochrona przed SCAM-em,
- 1.5.4. obrona przed phishingiem,
- 1.5.5. bezpieczeństwo stron www i przeglądarek,
- 1.5.6. ataki socjotechniczne z wykorzystaniem urządzeń,
- 1.5.7. ataki za pośrednictwem telefonu,
- 1.5.8. zagrożenia związane z urządzeniami mobilnymi,
- 1.5.9. zagrożenia związane z sieciami Wi-Fi,
- 1.5.10. zagrożenia w mediach społecznościowych,
- 1.5.11. dobre praktyki bezpieczeństwa,
- 1.5.12. prywatność, poufność i anonimowość w internecie.

1.6. Cechy szkolenia

- 1.6.1. Umożliwia monitorowanie postępu użytkownika.
- 1.6.2. Statusy lekcji: nierozpoczęta, w toku, ukończona.
- 1.6.3. Statusy modułu: nierozpoczęty, w toku, ukończony.
- 1.6.4. Statusy testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony.
- 1.6.5. Brak ustalonej kolejności kursu, użytkownik może od razu przejść do zaliczenia testu lub zapoznawać się z lekcjami video według uznania lub według narzuconego w organizacji harmonogramu.
- 1.6.6. Każdy moduł zawiera krótkie streszczenie zawartości.
- 1.6.7. Każda lekcja zawiera notatki w formie tekstowej.
- 1.6.8. Po ukończeniu materiału użytkownik wciąż ma do niego nieograniczony dostęp w ramach trwającej subskrypcji, przypisanej do organizacji.
- 1.6.9. Postęp w lekcji jest zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video.
- 1.6.10. Kurs umożliwia filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone).
- 1.6.11. Kurs pozwala użytkownikowi na ukrywanie ukończonych lekcji.
- 1.6.12. Po ukończeniu kursu użytkownik otrzymuje certyfikat (do wydruku).
- 1.6.13. Administrator platformy ma możliwość konfigurowania minimalnego postępu w kursie (tempa postępów) osiąganego przez użytkowników.
- 1.6.14. Szkolenie dostępne również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania.

1.7. Test

- 1.7.1. Składa się z pytań i odpowiedzi jednokrotnego wyboru.
- 1.7.2. Do testu można podejść przed ukończeniem lekcji video (dowolna kolejność wykonywania działań w obrębie kursu).
- 1.7.3. Administrator platformy ma możliwość konfigurowania progu punktowego wymaganego do zaliczenia testu.
- 1.7.4. Administrator platformy ma możliwość konfigurowania czasu, który musi upłynąć zanim użytkownik po raz kolejny może podejść do testu.
- 1.7.5. Test zapamiętuje odpowiedzi użytkownika (na wypadek opuszczenia testu przed ukończeniem).
- 1.7.6. Kolejność pytań i odpowiedzi jest losowana przed rozpoczęciem przez użytkownika testu.
- 1.7.7. Ukończenie/Zaliczenie testu wpływa na postęp ukończenia modułu.
- 1.7.8. Brak limitu czasowego na ukończenie testu.

- 1.7.9. Zmiana wymaganego w organizacji progu procentowego zaliczenia testu po ukończeniu przez użytkownika testu nie ma wpływu na status testu (zaliczony/niezaliczony).
- 1.7.10. Kurs zawiera test końcowy sprawdzający wiedzę z całego kursu.

2. ZARZĄDZANIE PLATFORMĄ

2.1. Zarządzanie użytkownikami

- 2.1.1. Podział na 3 role: właściciel konta - Administrator Główny - z uprawnieniami administratora, administrator, użytkownik.
- 2.1.2. Administrator Główny jest kontem zarządzającym platformą, zintegrowanym z zewnętrznym serwisem do zarządzania subskrypcją, który jest właścicielem subskrypcji.
- 2.1.3. Konto Administratora Głównego nie wlicza się do limitu użytkowników subskrypcji, ma dostęp do wszystkich funkcji platformy. Konto Administratora Głównego nie można usunąć, dezaktywować lub obniżyć uprawnień. Edycja danych Administratora Głównego wymaga zalogowania się do zewnętrznego serwisu do zarządzania subskrypcją.
- 2.1.4. Administrator jest rolą nadawaną przez Administratora Głównego lub innego Administratora, ma dostęp do wszystkich funkcji platformy, można go usunąć, dezaktywować lub obniżyć uprawnienia.
- 2.1.5. Użytkownik - ma dostęp do swojego pulpitu oraz szkolenia w platformie, nie może zarządzać platformą. Konto użytkownika może zostać utworzone ręcznie przez dowolnego administratora lub zaimportowanie z pliku .CSV.
- 2.1.6. Możliwość nadania funkcji menedżera grupy - wiąże się z rozszerzeniem widoczności użytkownika o członków grupy, którymi zarządza (wglądu do ich danych, postępów w nauce itd.).
- 2.1.7. Platforma pozwala na śledzenie postępów użytkowników w kursie (tylko dla Administratorów oraz Menedżerów).
- 2.1.8. Platforma wyświetla listę aktywności każdego użytkownika w organizacji wraz z informacją o dacie i rodzaju aktywności.

2.2. Właściwości użytkowników

- 2.2.1. Imię i nazwisko, e-mail oraz rola (administrator/użytkownik).
- 2.2.2. Wymóg unikalnego adresu e-mail w obrębie organizacji.
- 2.2.3. Możliwość dodawania użytkowników do platformy z poziomu interfejsu (formularz).
- 2.2.4. Możliwość masowego dodawania użytkowników do platformy poprzez import pliku .csv.
- 2.2.5. Możliwość aktualizacji danych użytkownika (imię i nazwisko) za pomocą importu .csv.
- 2.2.6. Importowany plik może mieć do 5000 wierszy (limit użytkowników).
- 2.2.7. Po dodaniu użytkownika do platformy, otrzymuje on wiadomość e-mail z zaproszeniem do organizacji i ustaleniem pierwszego hasła.
- 2.2.8. Administrator może dowolnie edytować dane wszystkich użytkowników (imię, nazwisko, adres e-mail, rola).
- 2.2.9. Administrator może dowolnie aktywować oraz dezaktywować konta wszystkich użytkowników.
- 2.2.10. Administrator może dowolnie usuwać konta wszystkich użytkowników.
- 2.2.11. Administrator ma dostęp do wszystkich funkcji w platformie.
- 2.2.12. Administrator ma dostęp do wszystkich zakładek w platformie.
- 2.2.13. Użytkownik ma dostęp do zakładki „Pulpit” oraz „Mój kurs”.
- 2.2.14. Menedżer ma rozszerzony dostęp do grup i użytkowników, którymi zarządza.

2.3. Zarządzanie grupami

- 2.3.1. Administrator może dowolnie tworzyć, edytować oraz usuwać grupy.



- 2.3.2. Każda grupa może mieć dokładnie 1 menedżera.
- 2.3.3. Menedżer nie może edytować grupy, którą zarządza.
- 2.3.4. Menedżer nie może dodawać lub usuwać użytkowników z grup, którymi zarządza.
- 2.3.5. Użytkownik może należeć do dowolnej liczby grup.
- 2.3.6. Menedżer nie musi być członkiem grupy, którą zarządza.

2.4. Ustawienia organizacji

- 2.4.1. Konfiguracja procentowego progu zdawalności testu.
- 2.4.2. Konfiguracja czasu przed kolejnym podejściem do testu.
- 2.4.3. Konfiguracja minimalnego wymaganego postępu w kursie (liczba ukończonych materiałów na tydzień).
- 2.4.4. Informacja o rodzaju subskrypcji (pełna/demo).
- 2.4.5. Informacja o czasie pozostałym do wygaśnięcia subskrypcji.
- 2.4.6. Wykres limitu użytkowników (użytkownicy w organizacji/limit subskrypcji).

2.5. Inne

- 2.5.1. Platforma posiada dedykowaną i stale aktualizowaną Bazę Wiedzy, w której znajdują się artykuły objaśniające najważniejsze funkcje platformy.
- 2.5.2. Motyw ciemny/jasny.
- 2.5.3. Comiesięczny newsletter dla użytkowników organizacji (wysyłany na adres e-mail użytkowników).

2.6. Wspierane przeglądarki:

- 2.6.1. Google Chrome,
- 2.6.2. Firefox,
- 2.6.3. Microsoft Edge.

3. SZKOLENIA DLA ADMINISTRATORÓW

- 3.1. Wykonawca zapewni szkolenie dla 5 administratorów z zakresu administrowania platformą szkoleniową.
- 3.2. Szkolenie musi obejmować minimum 4 godziny.
- 3.3. Szkolenie zostanie przeprowadzone w siedzibie urzędu lub zdalnie, z wykorzystaniem platform e-learningowych oraz narzędzi do zdalnego zarządzania.
- 3.4. Po zakończeniu szkolenia Wykonawca jest zobowiązany zapewnić możliwość konsultacji telefonicznych i mailowych z trenerem przez okres min. 14 dni.
- 3.5. Szkolenie będzie wyszczególnione jako osobna pozycja na wystawionej fakturze.

II. OPROGRAMOWANIE DO INWENTARYZACJI SPRZĘTU I OPROGRAMOWANIA

FUNKCJONALNOŚĆ	WYMAGANIA MINIMALNE
WYMAGANIA OGÓLNE	<ol style="list-style-type: none"> 1. Przedmiotem zamówienia jest zakup, wdrożenie oraz konfiguracja oprogramowania do kompleksowego monitoringu infrastruktury IT oraz inwentaryzacji sprzętu i oprogramowania w Urzędzie Miasta. W skład zamówienia wchodzi również wdrożenie i szkolenie administratorów IT w zakresie konfiguracji i zarządzania oprogramowaniem. 2. Licencje powinny obejmować możliwość instalacji zdalnych agentów na 220 stacjach roboczych. 3. Licencje powinny obejmować poniższe moduły oprogramowania: <ol style="list-style-type: none"> 3.1. Monitorowanie sieci i serwerów. 3.2. Inwentaryzacja sprzętu i oprogramowania. 3.3. Monitorowanie aktywności użytkowników. 3.4. Zarządzanie bezpieczeństwem danych i dostępem. 3.5. Helpdesk i zdalna pomoc techniczna. 4. Oprogramowanie ma zostać zainstalowane na serwerze urzędu, spełniającym minimalne wymagania techniczne wskazane przez producenta. 5. Zakres prac obejmuje: <ol style="list-style-type: none"> 5.1. Instalację serwera oprogramowania oraz konsoli zarządzającej. 5.2. Konfigurację zdalnych agentów na stacjach roboczych użytkowników. 5.3. Integrację oprogramowania z Active Directory. 5.4. Konfigurację polityk monitorowania infrastruktury sieciowej i serwerów. 5.5. Konfigurację alarmów oraz powiadomień e-mail/SMS w przypadku wykrycia incydentów lub awarii. 5.6. Konfigurację modułu HelpDesk do obsługi zgłoszeń użytkowników. 5.7. Testy wdrożeniowe i akceptacyjne w celu sprawdzenia poprawności działania systemu. 6. Wykonawca zobowiązuje się do przeprowadzenia szkolenia dla 5 administratorów IT z zakresu: <ol style="list-style-type: none"> 6.1. Instalacji i konfiguracji oprogramowania. 6.2. Zarządzania modułami monitoringu infrastruktury oraz inwentaryzacji. 6.3. Konfiguracji polityk monitorowania aktywności użytkowników. 6.4. Analizy logów i raportów generowanych przez system. 6.5. Obsługi modułu helpdesk i zdalnej pomocy technicznej. 7. Szkolenie musi trwać minimum 8 godzin i zakończyć się przekazaniem materiałów szkoleniowych w formie elektronicznej oraz papierowej. 8. Szkolenie zostanie przeprowadzone w siedzibie urzędu lub zdalnie, z wykorzystaniem platform e-learningowych oraz narzędzi do zdalnego zarządzania. 9. Po zakończeniu szkolenia Wykonawca jest zobowiązany zapewnić możliwość konsultacji telefonicznych i mailowych z trenerem przez okres min. 14 dni. 10. Szkolenie będzie wyszczególnione jako osobna pozycja na wystawionej fakturze. 11. Wsparcie techniczne i aktualizacje <ol style="list-style-type: none"> 11.1. Wykonawca musi zapewnić wsparcie techniczne oraz prawo do aktualizacji oprogramowania przez okres minimum 24 miesięcy od dnia wdrożenia. 12. Wsparcie techniczne musi obejmować możliwość zgłaszania problemów technicznych, zdalną pomoc oraz dostęp do aktualizacji oprogramowania.

PODSTAWOWE WYMAGANIA OPROGRAMOWANIA	<p>13. Oprogramowanie powinno posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.</p> <p>14. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwany użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji opensource (PostgreSQL w wersji 12 lub wyższej) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.</p> <p>15. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.</p> <p>16. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agentu, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agentu.</p> <p>17. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog</p>
MONITOROWANIE SIECI I SERWERÓW.	<p>18. MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalles w zakresie:</p> <p>18.1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping</p> <p>18.2. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)</p> <p>18.3. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci</p> <p>18.4. wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki</p> <p>18.5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.</p> <p>18.6. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku</p>

- 18.7. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- 18.8. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- 18.9. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- 18.10. zablokowania mapy urządzeń przed przypadkową edycją
- 18.11. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- 18.12. serwerów pocztowych:
 - 18.12.1. program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
 - 18.12.2. program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem)
 - 18.12.3. program ma możliwość wykonywania operacji testowych
 - 18.12.4. program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- 18.13. monitorowania serwerów WWW i adresów URL
- 18.14. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- 18.15. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- 18.16. obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np.
- 18.17. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- 18.18. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych ✓ monitoringu routerów i przełączników wg:
 - 18.18.1. zmian stanu interfejsów sieciowych
 - 18.18.2. ruchu sieciowego
 - 18.18.3. podłączonych stacji roboczych – graficzna prezentacja panelu switcha
 - 18.18.4. ruchu generowanego przez podłączone do portów stacje robocze
- 18.19. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/ zatrzymanie/ zrestartowanie
- 18.20. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- 18.21. wydajności systemów Windows:
 - 18.21.1. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy
19. Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
20. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych

	<p>ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0</p> <p>21. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).</p>
INWENTARYZACJA SPRZĘTU I OPROGRAMOWANIA	<p>22. W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:</p> <p>22.1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.</p> <p>22.2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.</p> <p>22.3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.</p> <p>22.4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.</p> <p>22.5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.</p> <p>22.6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).</p> <p>22.7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.</p> <p>22.8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.</p> <p>22.9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).</p> <p>22.10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.</p> <p>23. Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania:</p>

- 23.1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- 23.2. tworzenia powiązań między zasobami a urządzeniami,
- 23.3. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- 23.4. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- 23.5. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- 23.6. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- 23.7. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- 23.8. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- 23.9. importu danych z zewnętrznego źródła (.CSV),
- 23.10. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- 23.11. tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- 23.12. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutilizowany itp.,
- 23.13. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- 23.14. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- 23.15. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- 23.16. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- 23.17. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- 23.18. archiwizacji i porównywania audytów zasobów,
- 23.19. tworzenia kodów kreskowych dla zasobów,
- 23.20. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- 23.21. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- 23.22. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,

	<p>23.23.inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agentu poprzez manualne wykonanie skanów inwentaryzacji offline),</p> <p>23.24.definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencja/gwarancja”).</p> <p>24. Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</p> <p>24.1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.</p> <p>24.2. Informacje o aplikacjach używanych w organizacji.</p> <p>24.3. Tworzenie własnych wzorców aplikacji.</p> <p>24.4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.</p> <p>24.5. Informacje o komputerach, na których aplikacja została wykryta.</p> <p>24.6. Zarządzanie posiadanymi licencjami.</p> <p>24.7. Wskazywanie osób odpowiedzialnych za licencję.</p> <p>24.8. Wskazanie użytkowników licencji.</p> <p>24.9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.</p> <p>24.10.Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.</p> <p>24.11.Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.</p> <p>24.12.Zarządzanie posiadanymi licencjami: raport zgodności licencji.</p> <p>24.13.Możliwość przypisania do programów numerów seryjnych, wartości itp.</p> <p>25. Okna audytowe posiadają możliwość filtrowania elementów per oddział.</p>
ZDALNA POMOC	<p>26. PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.</p>

27. Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:
 - 27.1. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
 - 27.2. rozmowy również między „zwykłymi” użytkownikami
 - 27.3. przysyłanie plików między rozmówcami w trybie online
 - 27.4. tworzenie pokoi tematycznych, rozmów grupowych
 - 27.5. oznaczanie kontaktów jako „ulubionych” na liście kontaktów
 - 27.6. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
 - 27.7. może być wyświetlany w trybie jasnym lub ciemnym
28. W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
29. Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
30. Moduł pomocy zdalnej umożliwia również:
 - 30.1. pobieranie listy użytkowników z Active Directory,
 - 30.2. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
 - 30.3. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
 - 30.4. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
 - 30.5. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
 - 30.6. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
 - 30.7. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
 - 30.8. procesowanie zgłoszeń użytkowników z wiadomości e-mail,
 - 30.9. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
 - 30.10. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do
 - 30.11. wybranych kategorii zgłoszeń,
 - 30.12. wykonywanie operacji na wielu zgłoszeniach równocześnie,
 - 30.13. dołączanie załączników do zgłoszeń,
 - 30.14. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,

	<p>30.15.szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,</p> <p>30.16.wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,</p> <p>30.17.zrzuty ekranowe (podgląd pulpitu),</p> <p>30.18.zdalną modyfikację rejestrów,</p> <p>30.19.dystrybucję oprogramowania przez Agenty,</p> <p>30.20.definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,</p> <p>30.21.przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,</p> <p>30.22.dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),</p> <p>30.23.zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejowanie zadania dystrybucji pliku,</p> <p>30.24.możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,</p> <p>30.25.planowanie nieobecności pracowników helpdesk,</p> <p>30.26.obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np.</p> <p>30.27.przekroczeń SLA wraz z podsumowaniem,</p> <p>30.28.generowanie raportów obsługi helpdesk,</p> <p>30.29.zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),</p> <p>30.30.zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),</p> <p>30.31. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.</p>
PORTAL INFORMACYJNY W FORMIE PLATFORMY WWW	<p>31. Oprogramowanie posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:</p> <p>31.1. Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.</p> <p>31.2. Wyświetlana w trybie jasnym lub ciemnym (nocnym).</p> <p>32. Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.</p> <p>33. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:</p> <p>33.1. Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,</p> <p>33.2. Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,</p> <p>33.3. Statystyki z obszaru wydruków, Statystyki użycia aplikacji, Użycie łącza, Aktywność WWW,</p> <p>33.4. Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,</p> <p>33.5. Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem),</p> <p>33.6. Produktywność dla grupy, Statystyki czasu nieproduktywnego.</p>

OCHRONA PRZED USUNIĘCIEM	34. Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
FUNKcjONALNOŚĆ AGENTA	35. Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
INNE	<p>36. Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji.</p> <p>37. Program dostępny w języku polskim wraz z dokumentacją w języku polskim. Wsparcie techniczne świadczone telefonicznie lub mailowo w języku polskim.</p>
WDROŻENIE	<p>38. Instalacja centralnej konsoli zarządzającej: Oprogramowanie konsoli do zarządzania stacjami roboczymi zostanie zainstalowane na serwerze zamawiającego. System musi wspierać integrację z istniejącą infrastrukturą IT (m.in. Active Directory) oraz umożliwiać centralne zarządzanie politykami bezpieczeństwa dla wszystkich urządzeń.</p> <p>39. Instalacja oprogramowania na stacjach roboczych: Oprogramowanie agentów zostanie zainstalowane na co najmniej 100 stacjach roboczych zamawiającego. Agenci muszą zapewniać pełną ochronę antywirusową, filtrowanie ruchu sieciowego, blokowanie dostępu do nieautoryzowanych aplikacji oraz kontrolę urządzeń zewnętrznych (USB).</p> <p>40. Polityki bezpieczeństwa: Tworzenie i zarządzanie politykami: Oprogramowanie musi umożliwiać tworzenie polityk bezpieczeństwa, takich jak kontrola dostępu do urządzeń zewnętrznych, filtrowanie treści internetowych, monitorowanie aktywności użytkowników oraz kontrola dostępu do aplikacji.</p> <p>41. Szyfrowanie danych: System musi zapewniać szyfrowanie danych przesyłanych i przechowywanych na urządzeniach końcowych oraz chronić dane przed nieautoryzowanym dostępem.</p> <p>42. Monitorowanie w czasie rzeczywistym: System musi oferować monitorowanie zagrożeń i incydentów w czasie rzeczywistym, generowanie alertów oraz automatyczne raportowanie wykrytych naruszeń.</p> <p>43. Analiza zagrożeń: System musi umożliwiać przeprowadzanie analizy zagrożeń, w tym automatyczną kwarantannę oraz analizę podejrzanych plików w sandboxie.</p> <p>44. Zaimportowanie do systemu pliku CSV z danymi zawierającymi powiązania urządzeń z użytkownikami.</p> <p>45. Wykonawca zobowiązany jest do zapewnienia, że wdrożenie zostanie przeprowadzone zgodnie z najlepszymi praktykami branżowymi, a wszystkie działania zostaną dokładnie udokumentowane. W razie konieczności, wykonawca będzie zobowiązany do wsparcia technicznego podczas fazy testowej oraz początkowej eksploatacji systemu przez okres minimum 14 dni od zakończenia prac wdrożeniowych.</p>
SZKOLENIE DLA ADMINISTRATORÓW IT	<p>46. Szkolenie w formie warsztatów dla 3 administratorów IT obejmuje:</p> <p>46.1. Ogólne omówienie programu.</p> <p>46.2. Wymagania i instalacja systemu.</p> <p>46.3. Wstępna konfiguracja systemu i instalacja.</p> <p>46.4. Konfiguracja i praca w module monitorowanie infrastruktury.</p> <p>46.5. Konfiguracja i praca w module inwentaryzacji.</p> <p>46.6. Konfiguracja i praca w module obsługi użytkowników.</p> <p>46.7. Konfiguracja i praca w module zdalnej pomocy użytkownikom.</p> <p>46.8. Konfiguracja i praca w module ochrony danych przed wyciekiem.</p>

	<p>46.9. Konfiguracja i praca w Portalu informacyjnym.</p> <p>46.10. Rozwiązywanie najczęstszych problemów.</p> <p>47. Szkolenie musi obejmować minimum 16 godzin warsztatów.</p> <p>48. Szkolenie zostanie przeprowadzone stacjonarnie w miejscu wskazanym przez Wykonawcę lub zdalnie, z wykorzystaniem platform e-learningowych oraz narzędzi do zdalnego zarządzania.</p> <p>49. Jeżeli szkolenie odbędzie się w miejscu wskazanym przez Wykonawcę, zapewnia on nocleg dla uczestników szkolenia.</p> <p>50. Szkolenie musi się odbyć w ciągu 6 miesięcy od dnia podpisania umowy.</p> <p>51. Szkolenie kończy się egzaminem, po zdaniu którego uczestnik otrzyma stosowny certyfikat.</p> <p>52. Szkolenie będzie wyszczególnione jako osobna pozycja na wystawionej fakturze.</p>
--	---