Łukasiewicz
Instytut Technik Innowacyjnych
EMAG

OPIS PRZEDMIOTU ZAMÓWIENIA
„Dostawa oprogramowania oraz monitorów"
– nr postępowania FH/03/10/23

Oferowany przedmiot zamówienia musi spełniać wymagania określone przez Zamawiającego, tj. posiadać parametry i funkcjonalności nie gorsze (co najmniej takie same lub lepsze) od określonych poniżej.

Zamówienie podzielone jest na 8 części. Zamawiający dopuszcza składanie ofert częściowych.

Część nr 1 - Wsparcie do Oprogramowanie do nadzorowania 25 sesji uprzywilejowanych

Opis oprogramowania	**Oprogramowanie do nadzorowania sesji uprzywilejowanych**
Warunki licencji	1. Licencja nie może ograniczać ilości użytkowników, których w danym momencie sesje są nadzorowane, 2. Licencja powinna umożliwiać nadzorowanie dostęp do co najmniej 25 usług, 3. Wsparcie producenta, które obejmuje roczne aktualizacje oraz wsparcie liczone od dnia 31.12.2023. 4. Zamawiający posiada u siebie wdrożone rozwiązanie BeyondTrust Privilege Remote Access, zatem zaproponowane licencje mogą tyczyć się przedłużenia działania tego rozwiązania lub całkowicie nowego, równoważnego, spełniające opisywane funkcjonalności wraz z wdrożeniem
Cechy oprogramowania równoważnego	**Architektura** 1. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizujące funkcjonalności systemu. 2. System musi być zaprojektowany i przygotowany do umieszczenia w DMZ (hardening producenta). 3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia. 4. System musi umożliwiać tryb pracy awaryjnej zapewniający synchronizację danych między dwoma urządzeniami do uprzywilejowanego dostępu zdalnego, tworząc uproszczony

	proces bezpiecznej wymiany uszkodzonego urządzenia na zapasowe. 5. System musi umożliwiać nawiązywanie sesji przynajmniej w dwóch trybach: a) Z wykorzystaniem instalowanego agenta na systemie, do którego będzie nawiązywana sesja, b) Z wykorzystaniem serwerów proxy bez potrzeby instalacji agenta na systemie, do którego będzie nawiązywana sesja. 6. Serwery proxy (nawiązywanie sesji w sposób bezagentowy) muszą być zarządzane w sposób centralny z poziomu oprogramowania do uprzywilejowanego dostępu zdalnego (konfiguracja minimalnie w zakresie: nadawania uprawnień dostępowych do serwera proxy dla zewnętrznych dostawców, utworzenie serwera proxy, wyłączenie serwera proxy). 7. Komunikacja między elementami systemu do uprzywilejowanego dostępu zdalnego (tj. oprogramowaniem uprzywilejowanego dostępu zdalnego, agentami instalowanymi na urządzeniach końcowych oraz serwerami proxy) musi być szyfrowana (TLS) i odbywać się na jednym porcie 443. 8. Elementy systemu (agenci, serwery proxy, klienci) instalowani na zasobach i stacjach roboczych muszą umożliwiać pracę w trybie aktywnego nawiązywania połącznia z systemem uprzywilejowanego dostępu zdalnego, tj. bez pozostawiania otwartych portów nasłuchujących na urządzeniach końcowych. 9. System musi posiadać wsparcie dla protokołów SSH, RDP oraz VNC. 10. System musi posiadać możliwość rozbudowy o moduł obsługi sesji do aplikacji WEB (wbudowana przeglądarka WWW). 11. Systemu musi posiadać możliwość uruchomienia sesji aplikacyjnych (uruchomienie wskazanej aplikacji z serwera usług terminalowych lub uruchomienie aplikacji za pomocą dedykowanego agenta) 12. Systemu musi posiadać możliwość tunelowania protokołów TCP na zdefiniowanym porcie między komputerem zewnętrznego dostawcy a zarządzanym systemem. 13. System ma być dostarczony w polskiej wersji językowej (zarówno menu konfiguracyjne systemu jak i interfejs klientów, za pomocą których realizowane są sesje). **Funkcje operacyjne sytemu uprzywilejowanego dostępu zdalnego** 1. Logowanie do systemu uprzywilejowanego dostępu zdalnego musi odbywać się poprzez konta lokalne (tworzone na poziomie systemu do uprzywilejowanego dostępu zdalnego) lub konta i

	grupy importowane z Active Directory. 2. Logowanie dostawców zewnętrznych do systemu uprzywilejowanego dostępu zdalnego musi być zabezpieczone drugim składnikiem (2FA). 3. System musi realizować następujące scenariusze nawiązywania sesji przez zewnętrznego dostawcę: a) za pomocą klienta zainstalowanego na komputerze zewnętrznego dostawcy (gruby klient), b) za pomocą przeglądarki WWW z komputera zewnętrznego dostawcy (bez potrzeby instalacji klienta), c) za pomocą klienta zainstalowanego na urządzeniu mobilnym (minimum wsparcie dla systemu Android). 4. System musi umożliwiać opcję zastosowania przez kontraktora własnych klientów RDP i SSH. 5. System musi umożliwiać realizację sesji do stacji roboczych (przynajmniej Windows i Linux) i współdzielenie tej samej sesji między kontraktorem a operatorem pracującym przy stacji roboczej. 6. Rozpoczęcie sesji współdzielonej między kontraktorem a operatorem stacji roboczej musi podlegać procesowi akceptacji przez operatora stacji roboczej do której realizowana jest ta sesja. 7. Rozpoczęcie sesji przez zewnętrznego dostawcę musi podlegać kontroli dostępu poprzez: a) Wysyłanie powiadomień o zdarzeniu rozpoczęcia i zakończenia sesji przez zewnętrznego dostawcę do zdefiniowanej listy osób, b) Ograniczenie możliwości nawiązywania sesji przez zewnętrznych dostawców do określonych dni i godzin, oraz do określonych grup zasobów. c) Włącznie procesu wnioskowania przez zewnętrznego dostawcę o dostęp do zasobów i mechanizmu akceptacji lub odrzucenia wniosku przez właściciela zasobu. We wniosku muszą znaleźć się przynajmniej zakres dat, kiedy zewnętrzny dostawca będzie nawiązywał sesję oraz pole pozwalające opisać zakres wykonywanych przez niego prac. Wniosek musi być wysyłany w celu akceptacji do zdefiniowanej listy osób. 8. Konsola dostępowa dla zewnętrznego dostawcy musi posiadać co najmniej poniższe funkcje: a) widok grup zasobów z możliwością nawiązania sesji do tych zasobów (za pomocą menu kontekstowego

lub podwójnego kliknięcia), oraz możliwością wyszukiwania zasobów po ciągach znaków
   b) szczegółowy opis zasobu, do którego możliwe jest nawiązanie sesji, zawierający nazwę hosta / adres IP, status (aktywny/nieaktywny), typ systemu operacyjnego, edytowalną nazwę skróconą.
   c) funkcję wieloosobowego chatu działającą między uczestnikami sesji.
9. System musi umożliwić wyłączenie synchronizacji schowka i kopiowania plików między komputerem zewnętrznego dostawcy a zarządzanym zasobem.
10. System w trakcie sesji realizowanej przez zewnętrznego dostawcę musi umożliwiać:
   a) Dołączenie do sesji dodatkowych użytkowników posiadających konta w systemie uprzywilejowanego dostępu zdalnego;
   b) Dołączenie dodatkowych użytkowników do sesji nieposiadających konta w systemie uprzywilejowanego dostępu zdalnego przy jednoczesnej możliwości nałożenia dodatkowych restrykcji dla takiej osoby (minimum w zakresie odebrania kontroli myszy i klawiatury, automatyczne zakończenie sesji w przypadku braku połączenie autoryzowanego użytkownika ulegnie awarii);
   c) Przejęcie sesji zewnętrznego dostawcy przez uprawnioną osobę (audytora) i jej zakończenie.

Funkcje raportowania

1. System musi posiadać wbudowany i centralnie zarządzany moduł raportowy.
2. System musi generować centralnie konfigurowane i składowane raporty z przeprowadzonych sesji (łącznie z nagraniami sesji).
3. System musi rejestrować sesje graficzne oraz sesje z wierszem poleceń.
4. System musi umożliwiać wybór rozdzielczości rejestrowanych sesji.
5. W systemie muszą być dostępne raporty dotyczące co najmniej przeprowadzonych sesji i wykorzystania poświadczeń z wbudowanego magazynu haseł.
6. Raporty dotyczące przeprowadzonych sesji muszą podlegać

filtrowaniu co najmniej (wymagane wszystkie wymienione) w zakresie daty, nazwy użytkownika (zewnętrznego dostawcy), nazwy / adresu IP zarządzanego zasobu, grupy zarządzanych zasobów.

7. System musi posiadać możliwość uruchomienia filtrowania odbytych sesji po ciągach znaków pisanych z klawiatury w trakcie ich trwania.
8. W szczegółach raportu sesji muszą znajdować się co najmniej informacje na temat:
    a) daty rozpoczęcia i zakończenia sesji (długość trwania sesji),
    b) nazwy konta przechowywanego we wbudowanym magazynie haseł za pomocą którego zalogowano się do systemu,
    c) przesyłanych plików między maszyną zewnętrznego dostawcy a zarządzanym zasobem,
    d) nagrania z sesji (sesje graficzne oraz okna konsoli),
    e) transkrypcji chatu,
    f) wszystkich uczestników sesji (osoby, które dołączały do sesji w trakcie jej trwania),
    g) listy zdarzeń (log) dotyczący pracy narzędzia uprzywilejowanego dostępu zdalnego.

Konfiguracja i instalacja agentów

1. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi być przygotowany do masowej instalacji.
2. Plik instalacyjny agenta instalowanego na zarządzanym zasobie musi posiadać datę ważności, po upływie której niemożliwe będzie jego wykorzystanie.
3. Agent instalowany na zarządzanym zasobie musi być aktualizowany w sposób centralny z poziomu systemu uprzywilejowanego dostępu zdalnego.
4. System musi zapewniać możliwość określenia polityk aktualizacji agenta (możliwość definiowania co najmniej liczby jednocześnie aktualizowanych agentów oraz pasma przeznaczonego na aktualizację przez sieć).
5. System musi zapewnić możliwość zdefiniowania akcji zbierania dodatkowych danych na temat zdalnego hosta przez agenta, bez konieczności nawiązywania sesji (przynajmniej w zakresie zużycia CPU, nazwy zalogowanego użytkownika, zajętości dysku).

Wbudowany magazyn haseł

	1. System musi posiadać wbudowaną funkcjonalność magazynu poświadczeń (przechowywanie nazw kont i haseł, ukrywanie widoczności haseł przed zewnętrznymi dostawcami). 2. System musi umożliwiać dodawanie kont wykorzystywanych do zdalnego logowania co najmniej poprzez: a) wprowadzenie ręczne z poziomu interfejsu konfiguracyjnego narzędzia, b) wyszukanie i import z Active Directory, z możliwością automatycznej zmiany haseł na takich kontach. c) możliwość zintegrowania pobierania poświadczeń z systemu PAM (przynajmniej jednego), poświadczenia muszą być prezentowane w kontekście zasobu, do którego łączy się zewnętrzny dostawca (przy nawiązywaniu sesji musi być możliwość wyboru poświadczeń występujących wyłącznie na danym zasobie). 3. Użycie poświadczeń przez zewnętrznych dostawców musi podlegać kontroli dostępu. Uprawnienia do korzystania z danych poświadczeń (haseł) muszą być przyznawane dla pojedynczego konta dostawcy lub dla grupy kont dostawców. 4. Hasła przechowywane w magazynie haseł muszą być szyfrowane AES256 lub lepszym. **Integracje** 1. System musi posiadać otwarte API w zakresie pozwalającym na wykonanie integracji z oprogramowaniem firm trzecich. 2. System musi umożliwiać wykonanie integracji z systemami typu SIEM (syslog). 3. System musi umożliwiać wykonanie integracji z systemem PAM w zakresie pobierania z niego poświadczeń. 4. System musi umożliwiać wysyłanie powiadomień z wykorzystaniem SMTP. **Kontrola dostępu** 1. System musi posiadać możliwość zdefiniowania restrykcji sieciowych pozwalających ograniczyć dostęp do interfejsu zarządzającego oprogramowaniem przynajmniej w zakresie zdefiniowania adresów IP hostów lub adresów sieci znajdujących się na białej liście (liście dostępowej) i domyślnej akcji odrzucania innego ruchu skierowanego do interfejsu zarządzającego. 2. System musi umożliwiać edycję poziomu uprawnień użytkowników lub grup użytkowników co najmniej w zakresie: a) edycji grup zasobów w zakresie nadawania

	uprawnień dostępowych do zasobów dla zewnętrznych dostawców oraz uprawnień do edycji tych zasobów (zabronienie możliwości edycji zasobów w systemie uprzywilejowanego dostępu zdalnego), b) edycji i tworzenia nowych poświadczeń w magazynie haseł oraz do przyznawania uprawnień dla zewnętrznych dostawców do możliwości wykorzystania tych poświadczeń, c) generowania i podglądu raportów w tym nagrań z sesji, d) możliwości zapraszania do sesji dodatkowych użytkowników, e) możliwości odebrania lub nadania uprawnień do realizowania sesji z wykorzystaniem instalowanych agentów, serwerów proxy, protokołu RDP lub SSH. f) możliwości definiowania białych lub czarnych list poleceń w sesjach uruchamianych w konsoli.
Zakres wdrożenia dla rozwiązania równoważnego:	1. Inicjalizacja oprogramowania w środowisku Zamawiającego 2. Konfiguracja i instalacja agentów (5 sztuk na systemach Windows i Linux) lub utworzenie elementów połączeniowych (5 sztuk RDP oraz SSH) 3. Instalacja konsol dostępowych oraz ich konfiguracja 4. Skonfigurowanie integracji z domeną na potrzeby logowania do dostarczanego systemu 5. Konfiguracja i instalacja jump point jeśli jest dostępny 6. Konfiguracja sejfu haseł, import i tworzenie kont zarządzanych 7. Utworzenie do 3 grup użytkowników i nadanie uprawnień (role administratorzy, wnioskujący – firma zewnętrzna, pracownicy domowi) oraz skonfigurowanie uprawnień 8. Utworzenie polityk dla sesji 9. Testy odbiorcze konfiguracji 10. Opracowanie dokumentacji powdrożeniowej oraz instrukcji używania systemu dla użytkowników końcowych

Część nr 2 - Oprogramowanie do audytu środowiska ActiveDirectory dla 16 kontrolerów

Opis oprogramowania	Oprogramowanie do audytu środowiska ActiveDirectory
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 16 kontrolerów domeny ActiveDirectry; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 3. Zamawiający posiada obecnie rozwiązanie ManageEngine ADAudit Plus, Zamawiający oczekuje przedłużenie licencji i wsparcia na to rozwiązanie lub w przypadku zaproponowania rozwiązania alternatywnego to również usługę wdrożenia, które zapewni ten sam poziom funkcjonalności co obecne rozwiązanie oraz szkolenie dla administratorów i analityków SOC z nowego rozwiązania
Cechy oprogramowania	**Kluczowe funkcjonalności:** 1. System działa bezagentowo. 2. System działa na systemach z rodziny Windows. 3. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore. 4. System obsługuje integracje ze Splunk'iem i ArcSight'em 5. System działa w formie aplikacji Internetowej. 6. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych. 7. System działa na pojedynczej bazie danych. 8. System posiada wbudowane skrypty, które pozwalają na: a) backup bazy danych, b) odtworzenie bazy danych, c) zmianę bazy danych. 9. System używa jednego konta do połączenia z domeną. 10. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji. 11. System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego. 12. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące: a) Wszystkich zmian plików i folderów b) Plikach zmodyfikowanych c) Plikach usuniętych d) Plikach przeniesionych e) Plikach utworzonych 13. System umożliwia analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:

a) Nietypową aktywność danego użytkownika
b) Nietypową aktywność użytkownika na serwerze
c) Nietypową ilość prób np. logowań
d) Nietypowe godziny logowań użytkowników
e) Nietypowe działania na plikach

Funkcjonalności aplikacji:

1. System działa bezagentowo.
2. System obsługuje języki: Chiński, Japoński i Angielski.
3. System działa na systemach z rodziny Windows.
4. System pozwala na podłączenie certyfikatu, w formacie .PFX oraz Java keystore.
5. System obsługuje integracje ze Splunk'iem i ArcSight'em
6. System działa w formie aplikacji Internetowej.
7. System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
8. System działa na pojedynczej bazie danych.
9. System posiada wbudowane skrypty, które pozwalają na backup bazy danych, odtworzenie bazy danych, zmianę bazy danych.
10. System używa jednego konta do połączenia z domeną.
11. System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12. System posiada możliwość aktywacji podwójnej autentykacji techników oprogramowania.
13. System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego.
14. System umożliwia audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych
15. System posiada możliwość raportowania wszystkich domen z pomocą pojedynczego raportu.
16. System umożliwia zbiorcze audytowanie środowiska Active Directory oraz posiada wbudowane raporty dotyczące:
    a) Nieudanych próby zalogowania do środowiska domenowego
    b) Stacji roboczych
    c) Serwerów
    d) Kontrolerów domen
    e) Poprawne logowanie użytkowników wraz z pełną historią logowania
    f) Nieudane próby logowania na serwery Radius oraz historię logowań
    g) Zmiany dokonywane na kontach użytkowników, a w szczególności:
        - Tworzenie kont

	- Usuwanie kont - Dezaktywacja kont - Modyfikacja haseł - Spis zablokowanych użytkowników - Historie użytkowników h) Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup. i) Raportowanie użytkowników zagnieżdżonych w innych grupach. j) Raport aktywności użytkowników oraz dezaktywacji stacji roboczych przez wylogowanie lub wygaszacz ekranu. 17. Zmiany dokonane na obiektach komputerów, a w szczególności: a) Tworzenie kont b) Usuwanie kont c) Dezaktywację kont d) Historię kont 18. Audyt zmian w OU, a w szczególności a) Tworzenie OU b) Usuwanie OU c) Listę modyfikowanych OU d) Historię OU 19. Zmiany wartości OU oraz domen mogą zostać przesłane do ArcSight. 20. Audyt zmian w zasadach grupowych, a w szczególności: a) Tworzenie GPO b) Usuwanie GPO c) Listę zmodyfikowanych GPO d) Historia GPO 21. Zaawansowane raporty GPO mogą zostać przesłane do systemu SIEM 22. Zaawansowane zmiany w GPO 23. Audyt zmian uprawnień, a w szczególności: a) Uprawnienia dotyczące poziomu dostępu do domeny b) Uprawnienia zmian OU c) Uprawnienia zmian w kontenerach d) Uprawnienia zmian w GPO e) Uprawnienia zmian użytkowników f) Uprawnienia zmian grup g) Uprawnienia zmian komputerów h) Uprawnienia zmian DNS i) Zmiany w DNS'ach j) Śledzenie zmian nazw użytkowników/komputerów/grup 24. System pozwala na zbiorcze audytowanie zmian na serwerach plików, a w szczególności a) Windows

	b) Windows file Cluster c) EMC d) Net App e) Hitachi NAS 25. System posiada możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania 26. System obsługuje regex dla wzorców wykluczania plików. 27. System potrafi audytować wydruki, w tym: a) Kto wykonywał wydruk, b) Jaki plik drukował, c) Kiedy wykonał wydruk, d) Ile kopii wykonał, e) Jaki był rozmiar pliku, f) Ile stron pliku zostało wydrukowane, g) Użytą drukarkę, h) Na którym serwerze znajduje się drukarka 28. System pozwala na tworzenie raportów zgodności, a w szczególności posiada wbudowane raporty dotyczące: a) Raporty zgodności dla audytów, a w szczególności: b) SOX c) HIPAA d) PCI-DSS e) GLBA f) FISMA g) RODO/GDPR 29. System pozwala na audyt: a) Zmian na serwerach członkowskich b) Audyt stacji roboczych 30. System posiada moduł powiadomień w formie alertów a) Widocznych w systemie b) Drogą mailową c) Poprzez SMS 31. System umożliwia podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.) 32. System umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast. 33. System posiada alerty o przekroczonej przestrzeni dyskowej 34. Narzędzie umożliwia zwolnienie zajętej przestrzeni dyskowej 35. System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i ma możliwość dokładnego ustawiania czasu przeniesienia do archiwum. 36. System pozwala na audyt Azure Active Directory, a w szczególności: a) Poprawne logowanie użytkownika

	b) Niepoprawne logowanie użytkownika c) Niepoprawne logowanie użytkownika bazowane na nieprawidłowym podaniu hasła d) Aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej 37. System pozwala na audyt zmian na kontach użytkowników Azure Active directory, a w szczególności posiada wbudowane raporty dotyczące: a) Ostatnio utworzony użytkownik b) Ostatnio usunięty użytkownik c) Ostatnio zaktualizowany użytkownik d) Ostatnio aktywowany użytkownik e) Ostatnio dezaktywowany użytkownik f) Ostatnio zmienione hasło dla użytkownika g) Ostatnio zresetowane hasło dla użytkowników. 38. System pozwala na Audyt nadanych ról w Azure Active Directory, a w szczególności przygotowane raporty dotyczące: a) Ostatnio przypisany członek do roli b) Ostatnio odłączony członek od roli 39. System pozwala na audyt zmian grup w Azure Active Directory, a w szczególności: a) Ostatnio utworzona grupa b) Ostatnio usunięta grupa c) Ostatnio zaktualizowana grupa d) Ostatnio dodani członkowie do grup e) Ostatnio usunięci członkowie z grup 40. System umożliwia audyt plików na serwerach, w określonym odstępie czasowym bezagentowo lub w czasie rzeczywistym przy użyciu agenta, w tym posiada wbudowane raporty dotyczące: a) Wszystkich zmian plików i folderów b) Plikach zmodyfikowanych c) Plikach usuniętych d) Plikach przeniesionych e) Plikach utworzonych 41. Program posiada możliwość alertowania administratora w razie braku komunikacji z agentem. 42. System umożliwia audyt urządzeń USB dla Serwerów Windows 2016 i systemu Windows 10, a w szczególności posiada wbudowane raporty dotyczące: a) Zmiany na plikach lub folderach b) Odczyt danego pliku c) Zmiana danego pliku d) Kopiowane danego pliku 43. System umożliwia analitykę zachowań przy użyciu uczenia

	maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności: a) Nietypową aktywność danego użytkownika b) Nietypową aktywność użytkownika na serwerze c) Nietypową ilość prób np. logowań d) Nietypowe godziny logowań użytkowników e) Nietypowe działania na plikach 44. System posiada możliwość oceny ryzyka, opartego o uczenie maszynowe: a) Użytkownicy połączeni z dużą ilością zasobów b) Konta o dużej aktywności c) Konta o nadmiernej aktywności d) Konta z wysokim % niepowodzeń logowania e) Ostatnia aktywność użytkownika f) Uśpione konta administratorów g) Uprawnienia wykorzystane przez użytkowników h) Pierwsze użycie przydzielonego uprawnienia i) Konta oparte na zdalnym logowaniu 45. System obsługuje audytowanie zmian na share'ach sieciowych, w tym posiada przygotowane raporty dotyczące: a) Zmiany nazw plików oraz folderów b) Utworzenie nowych plików oraz folderów c) Usunięcie plików oraz folderów d) Przeniesienie plików oraz folderów e) Zmiany uprawnień na plikach i folderach 46. System umożliwia przesyłanie logów do SYSLOG'a lub innych systemów SIEM'owych. 47. System obsługuje połączenie LDAP'owe po SSL'u. 48. System pozwala na eksportowanie raportów/danych do formatów: a) CSV b) PDF c) XLS d) HTML 49. System dostarcza informacje o bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów. 50. System dodatkowo obsługuje raportowanie z ADLDS oraz LAPS'a. 51. System potrafi przetworzyć dane do systemu SIEM'owego, w formacie RFC 3164 lub RFC 5424, a) W tym obsługuje wysyłanie danych po UDP jak i TCP. 52. System potrafi archiwizować dane do plików .zip oraz dołączać je do bazy danych, na żądanie administratora. a) W tym, system pozwala na archiwizację wybranej kategorii zdarzeń.

	53. System potrafi zaimportować pliki .evt oraz .evtx, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych. 54. System pozwala na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą. 55. System pozwala na uruchomienie dowolnego programu, w momencie wystąpienia alertu. 56. System obsługuje wiele domen na pojedynczej instancji. 57. System pozwala na pobieranie danych z AzureAD, w tym przetworzenia ich wg. własnych wbudowanych reguł. 58. System posiada możliwość wyszukiwania własnych, wbudowanych raportów, na podstawie słów kluczowych. 59. System posiada możliwość śledzenia wiersza poleceń użytych przez proces. 60. System umożliwia konfigurację wysokiej wydajności. 61. System posiada raport zmian uprawnień NetApp i EMC w celu dostarczenia informacji o wartościach uprawnień przed i po. 62. System posiada możliwość konfiguracji ustawień agenta. 63. System umożliwia pojedyncze logowanie (SSO) za pośrednictwem NTLM lub SAML. 64. System pozwala na prezentację wszystkich działań użytkowników w jednym raporcie w obszarze Account Management. 65. System umożliwia przeprowadzenie audytu i raportu na temat wykorzystania podatnego na Netlogon połączenie Schannel przez urządzenia z systemem Windows. 66. System pozwala kontrolować dostęp do plików i zmiany uprawnień w systemach pamięci masowej Huawei OceanStor.

Część nr 3 - Narzędzie do śledzenia błędów oraz zarządzania projektem

Opis oprogramowania	Narzędzie do śledzenia błędów oraz zarządzania projektem
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 200 użytkowników; 2. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 3. Zamawiający posiada obecnie rozwiązanie Jira Software Cloud Standard, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Jira Software Cloud Standard do rozwiązania przedstawionego w ofercie
Cechy oprogramowania	1. Oprogramowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi realizować funkcjonalność narzędzia do śledzenia zadań (issue tracking) 3. Oprogramowanie musi realizować funkcjonalność narzędzia do zarządzania błędami (Bug tracking); 4. Oprogramowanie musi zapewniać możliwość zarządzania wieloma różnymi projektami; 5. Oprogramowanie musi zapewniać wsparcie dla kompleksowego zarządzania projektem i metod typu Agile (Agile Project Management); 6. Oprogramowanie musi zapewniać możliwość dowolnej konfiguracji przepływu pracy (workflow); 7. Oprogramowanie musi pozwalać integracja z popularnymi platformami programistycznymi jak Eclipse, IntelliJ IDEA, Microsoft Visual Studio, Microsoft Visual Studio Code, JDeveloper, NetBeans, Zend Studio, inne; 8. Oprogramowanie musi zapewniać możliwość zarządzania błędami, właściwościami projektu, zadaniami, osiągnięciami lub innymi zagadnieniami; 9. Oprogramowanie musi zapewniać możliwość połączenia tworzonych zadań i zgłoszeń z kodem źródłowym, dostęp do kodu źródłowego; 10. Oprogramowanie musi zapewniać możliwość dodawania załączników; 11. Oprogramowanie musi zapewniać możliwość tworzenia nowych zadań za pośrednictwem przeglądarki, poczty elektronicznej oraz zintegrowanego środowiska programistycznego (IDE); 12. Oprogramowanie musi zapewniać możliwość szeregowania zadań, nadawania priorytetów; 13. Oprogramowanie musi zapewniać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 14. Oprogramowanie musi zapewniać możliwość generowania

	powiadomień członków zespołu projektowego z możliwością ich konfiguracji; 15.Oprogramowanie musi zapewniać możliwość tworzenia ról, poziomów uprawnień, grup użytkowników; 16.Oprogramowanie musi zapewniać możliwość tworzenia użytkowników, przydzielanie ról, poziomów uprawnień dla grup użytkowników; 17.Oprogramowanie musi zapewniać możliwość definiowania uprawnień dostępu z poziomu panelu; 18.Oprogramowanie musi zapewniać możliwość synchronizacji katalogu użytkowników z systemem uwierzytelniania opisanym w poniższym dokumencie oraz LDAP; 19.Oprogramowanie musi zapewniać możliwość rejestracji historii aktywności użytkowników – dostęp do ostatnio otwartych zadań, projektów; 20.Oprogramowanie musi zapewniać możliwość wyszukiwania pełnotekstowego, filtrowania i raportowania; 21.Oprogramowanie musi zapewniać możliwość generowania zestawień i statystyk podsumowujących realizacje projektu; 22.Oprogramowanie musi zapewniać możliwość generowania dokumentów w formacie xls, xlsx, xlsm, doc,docx; 23.Oprogramowanie musi zapewniać możliwość wyświetlania podsumowań i raportów dla rozpoczętych projektów – ostania aktywność, kamienie milowe, logi zmian, mapy projektu, wykresy;
Inne wymagania	1. Oprogramowanie musi być dostarczone w najnowszej dostępnej wersji; 2. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi zapewniać możliwość integracji z narzędziem do repozytorium kodu źródłowego dostarczonym w niniejszym postępowaniu 4. Możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git); 5. Dostępność aplikacji mobilnej na system Android i IOS.

Część nr 4 - Narzędzie do repozytorium kodu źródłowego

Opis oprogramowania	Narzędzie do repozytorium kodu źródłowego
Warunki licencji	1. Pakiet licencji musi zawierać prawo do korzystania dla min. 100 użytkowników; 2. Licencja musi zawierać prawo do instalacji na własnym serwerze. 3. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 4. Zamawiający posiada obecnie rozwiązanie Bitbucket Datacenter, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Bitbucket Datacenter do rozwiązania przedstawionego w ofercie
Cechy oprogramowania	1. Oprogramowanie musi posiadać interfejs użytkownika dostępny przez przeglądarkę internetową; 2. Oprogramowanie musi posiadać funkcjonalność narzędzia kontroli wersji kodu źródłowego, 3. Oprogramowanie musi posiadać funkcjonalność narzędzia repozytorium kodu źródłowego, dokumentów, witryn i innych plików; 4. Oprogramowanie musi posiadać możliwość przeglądania kodu źródłowego, dokumentów, witryn i katalogu innych dokumentów; 5. Oprogramowanie musi posiadać możliwość zarządzania prawami dostępu do publikowanych materiałów; 6. Oprogramowanie musi posiadać możliwość zakładania nieograniczonej liczby prywatnych repozytoriów dla każdego z użytkowników; 7. Oprogramowanie musi posiadać możliwość automatycznego generowania plików README na podstawie plików podobnych do plików Markdown; 8. Oprogramowanie musi posiadać funkcjonalność narzędzia do śledzenia problemów (Issue tracking); 9. Oprogramowanie musi posiadać możliwość budowania oprogramowania; 10. Oprogramowanie musi posiadać możliwość śledzenia zmian w komponentach i wersjach oprogramowania; 11. Musi istnieć możliwość logowania do serwera SYSLOG.
Inne wymagania	1. Oprogramowanie w najnowszej dostępnej wersji; 2. Oprogramowanie musi posiadać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 3. Oprogramowanie musi posiadać dostępność interfejsu REST API; 4. Oprogramowanie musi posiadać oprogramowanie oparte na Git; 5. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem do śledzenia błędów i zarządzania projektem opisanym w niniejszym projekcie, w zakresie pozwalającym na śledzenie i edytowanie błędów i problemów, powiązań pomiędzy

	problemami a kodem źródłowym; 6. Oprogramowanie musi posiadać możliwość instalacji oprogramowania na serwerze pracującym pod kontrolą systemu operacyjnego Linux; 7. Oprogramowanie musi posiadać możliwość integracji z systemami kontroli wersji (minimum z: Subversion, Mercurial, Git); 8. Oprogramowanie musi zapewniać możliwość integracji z Narzędzia do śledzenia błędów oraz zarządzania projektem

Część nr 5 - Oprogramowanie do obróbki plików multimedialnych i graficznych

Przedmiotem zamówienia jest zakup 16 szt. licencji oprogramowania Adobe Creative Cloud lub równoważnego spełniającego poniżej wskazane parametry równoważności.

Opis równoważności:

1. Oprogramowanie do tworzenia grafiki, animacji, video oraz treści internetowych. Oprogramowanie powinno umożliwiać:

a. tworzenie i obróbkę grafiki wektorowej
b. tworzenie i obróbkę grafiki rastrowej
c. obróbkę zdjęć
d. tworzenie kompozycji wektorowych
e. opracowywanie, tworzenie i udostępnianie prototypów interfejsu użytkownika
f. obróbkę materiałów w natywnych formatach, a także tworzenie produkcji filmowych, telewizyjnych i internetowych
g. tworzenie animacji i efektów wizualnych na potrzeby filmów, telewizji, wideo i stron internetowych
h. tworzenie fotorealistycznych obrazów 3D do oznaczeń marki, ujęć produktów i projektów opakowań
i. projektowanie i programowanie, aktywnych witryn www
j. kompleksową obsługę plików PDF z dowolnego miejsca

2. Licencje czasowe (1 rok), wersja przypisana do stacji roboczej

Część nr 6 - Oprogramowanie do inwentaryzacji środowiska IT dla 400 zasobów z wbudowanym narzędziem do połączeń zdalnych dla 250 zasobów i 5 techników

Oprogramowanie do inwentaryzowania

1. Kluczowe funkcjonlności

1.1. Rozwiązanie jest systemem heterogenicznym i posiada możliwość instalacji na systemie operacyjnym Windows x64, jak również Linux,

1.2. Rozwiązanie jest instalowane z własną darmową bazą danych postgreSQL, z możliwością migracji do komercyjnej bazy danych MS SQL,

1.3. Rozwiązanie wspiera integrację Active Directory, LDAP

1.3.1. Rozwiązanie pozwala na import grup z AD

1.4. Rozwiązanie posiada własny wbudowany interfejs, przez który odbywa się konfiguracja bazy danych

1.5. Rozwiązanie integruje się z dowolną skrzynką pocztową działająca na protokole POP, POPS, IMAP, IMAPS, SMTP, SMTPS, jak również obsługuje Exchange Web Services (EWS),

1.6. Rozwiązanie wspiera możliwość logowania bez potrzeby ponownego używania poświadczeń do aplikacji dzięki autentykacji poprzez SAML 2.0 Single Sign On (SAML SSO),

1.7. Aplikacja posiada możliwość uruchomienia dwuskładnikowego logowania przy użyciu Emaila lub google Authenticator'a

1.8. Aplikacja pozwala na podpięcie certyfikatów SSL

1.9. Aplikacja działa na bazie dostępnych ról uprawniających do pracy w narzędziu

2. Możliwości oprogramowania:

2.1. Rozwiązanie posiada natywną integracje z innymi produktami ManageEngine - umożliwia połączenie z Endpoint Central

2.2. Rozwiązanie posiada własny wbudowany moduł raportowania wzbogacony o możliwość kwerendowania do bazy danych,

2.3. Rozwiązanie wspiera przeglądarki – IE Edge, Chrome, Firefox

2.4. Dostęp do systemu dla użytkownika jest zapewniony za pośrednictwem konsoli webowej lub z aplikacji mobilnej

3. Ogólne wymagania dotyczące funkcjonalności produktu:

3.1. Rozwiązanie posiada Centralną bazę zasobów, oprogramowania oraz bazę CMDB wraz ze zintegrowanym wykrywaniem środowiska IT

3.2. Rozwiązanie umożliwia przechowywanie danych o wszystkich jednostkach konfiguracji (CI) takich jak:

3.2.1. Komputery

3.2.2. Drukarki sieciowe

3.2.3. Urządzenia sieciowe

3.2.4. Pakiety oprogramowania

3.2.5. Komponenty komputerów i urządzeń sieciowych

3.2.6. Usługi biznesowe oraz IT

3.2.7. Zasoby ludzkie (np. użytkownicy, grupy użytkowników, serwisanci, grupy serwisowe)

3.3. Rozwiązanie zawiera gotowy schemat danych wraz z listą możliwych relacji pomiędzy jednostkami konfiguracji, jak również możliwość rozbudowanie go o własne, zdefiniowane relacje

3.4. Rozwiązanie umożliwia dynamiczne rozszerzenie schematu danych o dodatkowe atrybuty, w tym atrybuty dedykowane dla konkretnego typu jednostki konfiguracji CI. Rozszerzenie odbywa się z poziomu interfejsu graficznego systemu
3.5. Rozwiązanie umożliwia przedstawienie w sposób graficzny wzajemnych relacji pomiędzy jednostki konfiguracji CI.
3.6. Rozwiązanie umożliwia przechowywanie informacji pomiędzy incydentami, problemami oraz zmianami, a jednostkami konfiguracji
3.7. Rozwiązanie umożliwia ręczne dodawanie jednostek konfiguracji oraz relacji pomiędzy nimi z poziomu interfejsu graficznego jak również importu danych o jednostkach konfiguracji z plików w formacie CSV lub XML
3.8. Rozwiązanie posiada zintegrowany moduł wykrywania środowiska IT, pozwalający na wykrycie co najmniej konfiguracji komputerów, serwerów i oprogramowania. Wykrywanie opiera się na wykorzystaniu skanowania agentowego.
3.9. Rozwiązanie umożliwia przechowywanie informacji o poszczególnych elementach konfiguracji w taki sposób, by możliwe było rejestrowanie i śledzenie historii posiadania elementu konfiguracji przez użytkowników, powiązanie z nim informacji o koszcie zakupu, innych kosztach eksploatacyjnych, warunkach umowy serwisowej, dostawcą
3.10. Rozwiązanie umożliwia wyszukiwanie elementów konfiguracji po dowolnych atrybutach, zarówno standardowych, jaki i dodanych przez użytkownika, w tym po kodach kreskowych
3.11. Rozwiązanie umożliwia zdefiniowanie wartości początkowej elementu konfiguracji oraz mierzenie jego amortyzacji.
3.12. Rozwiązanie umożliwia powiązanie poszczególnych elementów konfiguracji z danymi użytkownika (jego imieniem i nazwiskiem, nr telefonu, departamentem), departamentu, innymi elementami konfiguracji i katalogiem usług.
3.13. Rozwiązanie umożliwia przechowywanie informacji o posiadanych przez użytkownika licencjach na oprogramowanie, powiązać posiadane licencje z zainstalowanym na komputerach oprogramowaniem oraz rejestrować historię zmian posiadania danej licencji
3.14. Rozwiązanie umożliwia zarządzanie licencjami na oprogramowanie posiadane przez użytkowników w tym zarządzanie umowami dotyczącymi zakupu licencji oraz zasilanie CMDB danymi dotyczącymi licencji pochodzącymi z innych źródeł danych.
3.15. Rozwiązanie umożliwia wygenerowanie raportu posiadanych licencji przez użytkownika oraz raportów zgodności licencji z zainstalowanym oprogramowaniem
3.16. Rozwiązanie umożliwia z poziomu interfejsu oprogramowania nawiązanie sesji zdalnej w trybie przejęcia pulpitu użytkownika z komputerem przechowywanym w bazie
3.17. Rozwiązanie posiada API
3.18. Rozwiązanie posiada moduł wykrywania środowiska, który umożliwia zbieranie danych o konfiguracji komputerów, co najmniej:
3.18.1. Ilości i rodzaju procesora
3.18.2. Wielkość dostępnej pamięci fizycznej i wirtualnej
3.18.3. Nr seryjnego komputera
3.18.4. Nazwa i wersja systemu operacyjnego
3.18.5. Zainstalowane oprogramowanie i poprawki
3.19. Rozwiązanie posiada mechanizm generowania kodów kreskowych dla zasobów. Moduł pozwala na zdefiniowanie formatu kodu kreskowego i jego wydruk według zdefiniowanego formatu wydruku.

3.20. Rozwiązanie posiada możliwość wprowadzania zasobów skanowanych po kodzie kreskowym
3.21. Rozwiązanie umożliwia przeprowadzenie wykrywania zmian w konfiguracji i generowania raportów porównawczych zmian w elementach konfiguracji
3.22. Rozwiązanie umożliwia przeprowadzenie automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu 3.
23. Rozwiązanie umożliwia przeprowadzenie skanowania komputerów i zasilenie danych do bazy dla komputerów niepodłączonych do sieci komputerowej. Możliwe jest zastosowanie specjalnych skryptów, których plik wynikowy następnie zostanie zaimportowany do bazy.
3.24. System posiada możliwość zarządzania umowami serwisowymi dla elementów konfiguracji (CI) przechowywanych w bazie konfiguracji CMDB
3.25. Rozwiązanie w ramach zarządzania umowami posiada możliwość tworzenia umów, przegląd, edycje oraz usuwanie
3.26. Moduł zarządzania umowami serwisowymi umożliwia rejestrację warunków umów gwarancyjnych i serwisowych, w tym w szczególności dane teleadresowe gwaranta, czas obowiązywania umowy, jej koszt, warunki na jakich umowa jest świadczona oraz powiązania ich z jednym lub wieloma elementami konfiguracji bazy CMDB
3.27. Moduł zarządzania umowami serwisowymi posiada funkcjonalność pozwalającą przesyłać powiadomienia o wygaśnięciu okresu obowiązywania umowy serwisowej i gwarancyjnej
3.28. Rozwiązanie w ramach zarządzania umowami posiada możliwość dołączenia załączników
3.29. Rozwiązanie w ramach zarządzania umowami posiada możliwość tworzenia tzw. Umów podrzędnych do głównej umowy.
3.30. Rozwiązanie w ramach zarządzania umowami pozwala na tworzenie dodatkowych pól niezbędnych i wymaganych przez organizacje
3.31. Moduł zarządzania zakupami umożliwia przeprowadzenie procesu zakupowego składającego się z co najmniej następujących kroków:
3.31.1. Utworzenie zamówienie – rejestracja numeru zamówienia, powiązanie z dostawcą, określenie terminu realizacji zamówienia
3.31.2. Dodanie pozycji do zamówienia – rejestracja produktów, ich ilości oraz ceny jednostkowej produktu
3.31.3. Przedstawienie zamówienia do akceptacji – moduł zarządzania zakupami umożliwia przeprowadzenie weryfikacji i akceptacji zamówienia przez osoby trzecie, z tymże użytkownik rejestrujący zamówienie nie może być jednocześnie osobą trzecią weryfikującą i akceptującą realizację zamówienia
3.31.4. Powiązanie zamówienia z elementami konfiguracji w bazie CMDB
3.31.5. Moduł zarządzania zakupami umożliwia przesłanie powiadomienia do osób trzecich o przekroczonym terminie realizacji zamówienia
3.32. Aplikacja pozwala zarządzać procesem wypożyczenia sprzętu
3.33. Aplikacja pozwala na budowanie i nadzorowanie magazynu sprzętu
3.34 Aplikacja pozwala na generowanie grup w oparciu o kryteria

Część nr 7 - Oprogramowanie do zgłaszania i zarządzania problemami informatycznymi użytkowników końcowych (helpdesk)

Opis oprogramowania	**Oprogramowanie do zgłaszania i zarządzania problemami informatycznymi użytkowników końcowych (helpdesk)**
Warunki licencji	4. Pakiet licencji musi zawierać prawo do korzystania dla min. 15 pracowników helpdesk, którzy mają mieć możliwość rozwiązywania zgłaszanych problemów; 5. Pakiet licencji musi zawierać prawo do korzystania przez nieograniczoną ilość użytkowników, chcących zgłaszać problemy ze swoim stanowiskiem komputerowym i oprogramowaniem na nim; 6. Wsparcie producenta, które obejmuje aktualizacje oraz wsparcie przez okres 12 mc. aktywności subskrypcji. 7. Zamawiający posiada obecnie rozwiązanie Jira Service Management Cloud Standard, w przypadku zaproponowania innego rozwiązania, Wykonawca zobowiązany jest do migracji danych z obecnego rozwiązania Jira Service Management Cloud Standard do rozwiązania przedstawionego w ofercie
Cechy oprogramowania	24.Oprogramowanie musi udostępniać podstawowy interfejs użytkownika dostępny przez przeglądarkę internetową; 25.Oprogramowanie musi posiadać portal samoobsługowy, tj. bazę wiedzy w której użytkownicy mogą samodzielnie znaleźć rozwiązanie swojego problemu 26.Oprogramowanie musi umożliwiać rejestrację zgłoszeń poprzez wysłanie do niego maila od użytkownika 27.Oprogramowanie musi umożliwiać tworzenie formularzy i powiązane z nimi przepływy pracy do zgłaszania i obsługi zgłoszeń 28.Oprogramowaniem musi posiadać kolejki zgłoszeń, które można wykorzystać do priorytezowania zadań 29.Oprogramowanie musi umożliwiać zarządzanie i nadzorowanie SLA realizowanych zgłoszeń 30.Oprogramowanie musi posiadać gotowe raporty oraz możliwość tworzenia własnych, poprzez które będzie można uzyskać informację nt. czasów rozwiązania zadań czy wskaźnika SLA 31.Oprogramowanie musi posiadać mechanizmy automatyzujące część prac pracowników helpdesk, aby przyspieszyć realizację zadań 32.Oprogramowanie musi posiadać gotowe szablony do zarządzania usługami 33.Oprogramowanie ma posiadać przestrzeń na pliki o wielkości min 200GB 34. Oprogramowanie ma umożliwiać lub mieć oficjalnie ogłoszoną funkcjonalność prowadzenia rozmów między pracownikiem helpdesk, a pracownikiem zgłaszającym błąd poprzez stosowane u zamawiającego oprogramowanie Microsoft Teams 35.Oprogramowanie ma umożliwiać wysyłanie nieograniczonej ilości alertów i powiadomień drogą e-mail oraz SMS 36.Oprogramowanie ma umożliwiać eskalację zgłoszeń 37.Oprogramowanie musi umożliwiać zarzadzanie dyżurami domowymi 38.Oprogramowanie ma posiadać rejestr usług, aby móc mierzyć jakość ich realizacji 39.Oprogramowanie ma umożliwiać zarządzanie zmianami

	40. Oprogramowanie ma posiadać dziennik w którym są rejestrowane wszystkie istotne zmiany administracyjne w oprogramowaniu jak np. zmiana uprawnień
Inne wymagania	6. Oprogramowanie musi być dostarczone w najnowszej dostępnej wersji; 7. Oprogramowanie musi zapewniać możliwość instalacji wtyczek (ang. plug-in), rozszerzających funkcjonalność oprogramowania; 8. Oprogramowanie musi zapewniać możliwość integracji z posiadanym narzędziem Jira Software; 9. Jeśli oferowane oprogramowanie jest dostarczane jako produkt chmurowy, musi istnieć możliwość zdefiniowania, aby dane przechowywane były na terenie Unii Europejskiej; 10. Dostępność aplikacji mobilnej na system Android i IOS.

Część nr 8 – Monitory

Parametry nie mniejsze niż:

- Zastosowanie: Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu, poczty elektronicznej oraz systemu SIMPLE.ERP
- Przekątna ekranu: 23.8”
- Rodzaj matrycy: LED, TFT, VA
- Rozdzielczość ekranu: 1920 x 1080
- Format obrazu: 16:9
- Częstotliwość odświeżania ekranu: 75Hz
- Liczba wyświetlanych kolorów: 16,7 ml
- Czas reakcji plamki: 5 ms – 12 ms
- Kontrast: 3000:1
- Jasność: 250 cd/m²
- Kąt widzenia pion: 178 °
- Kąt widzenia poziom: 178 °
- Porty wejścia/wyjścia: HDMI x 1, VGA x 1
- Wielkość plamki: 0,2745mm
- Możliwość montażu na ścianie: tak / Standard VESA 100x100 mm
- Informacje dodatkowe: regulacja pochylania w pionie
- Standardowe zużycie energii: 15,7W
- Maksymalne zużycie energii: 24W
- Wyposażenie: instrukcja obsługi, kabel HDMI
- Gwarancja: nie mniejsza niż 36 miesięcy