OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu kontroli dostępu do sieci (NAC) dla sieci IT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji dożywotniej (bezterminowej) systemu kontroli dostępu do sieci klasy NAC (Network Access Control), zwanego dalej „Systemem", przeznaczonego do ochrony sieci ITZamawiającego (przewodowej i bezprzewodowej), wraz z 12-miesięczną licencją wsparcia technicznego producenta oprogramowania, wdrożeniem Systemu oraz szkoleniem dla 2 osób w wymiarze 4 godzin.

1.2. Zakres ilościowy zamówienia:

Lp.	Element przedmiotu zamówienia	Ilość
1	Licencja dożywotnia (bezterminowa) Systemu NAC na co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości), z możliwością rozbudowy do co najmniej 200 – zgodnie z rozdz. 4	1 kpl.
2	Licencja wsparcia technicznego producenta oprogramowania na okres 12 miesięcy – zgodnie z rozdz. 7	1 kpl.
3	Usługa wdrożenia Systemu w sieci biurowej Zamawiającego – zgodnie z rozdz. 5	1 usługa
4	Szkolenie z administrowania Systemem – 4 godziny zegarowe, 2 osoby, forma stacjonarna lub zdalna – zgodnie z rozdz. 6	1 usługa

1.3. Kody CPV: 48000000-8 Pakiety oprogramowania i systemy informatyczne; 48730000-4 Pakiety oprogramowania zabezpieczającego; 72263000-6 Usługi wdrażania oprogramowania; 80533100-0 Usługi szkolenia komputerowego.

2. Opis środowiska Zamawiającego

2.1. System zostanie wdrożony w sieci biurowej Zamawiającego. Środowisko obejmuje w szczególności:

- liczbę stanowisk pracy i użytkowników: do 50; szacunkowa liczba urządzeń końcowych (komputery, drukarki, telefony VoIP, urządzenia mobilne, inne): 100;
- przełączniki sieciowe: tak
- kontroler Wi-Fi / punkty dostępowe (producent, model, liczba), SSID: tak;
- platforma wirtualizacyjna przeznaczona dla Systemu: tak;
- zapora sieciowa / koncentrator VPN: UTM; tak
- system SIEM / serwer Syslog: w trakcie wdrażania.

2.2. Szczegółowe informacje o konfiguracji sieci zostaną przekazane Wykonawcy po zawarciu umowy i podpisaniu zobowiązania do zachowania poufności.

3. Wymagania ogólne

3.1. Wykonawca dostarczy licencje nowe, nieużywane i nieaktywowane wcześniej na żadnym urządzeniu ani koncie użytkownika, pochodzące z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, udzielone na rzecz Zamawiającego.

3.2. Licencja Systemu musi być dożywotnia (bezterminowa). Po upływie okresu wsparcia technicznego producenta System musi zachować pełną funkcjonalność w zakresie dostarczonej wersji, bez ograniczenia liczby obsługiwanych autoryzacji.

3.3. Zamawiający zapewni zasoby infrastruktury wirtualizacyjnej dla Systemu. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe (vCPU, RAM, przestrzeń dyskowa) dla oferowanej konfiguracji, w tym dla instalacji rozproszonej i mechanizmu Disaster Recovery.

3.4. Wszystkie licencje niezbędne do realizacji wymagań z rozdz. 4 muszą być dostarczone w ramach zamówienia. Zamawiający nie dopuszcza konieczności zakupu dodatkowych licencji lub modułów w celu spełnienia wymagań, z wyjątkiem licencji rozszerzających liczbę autoryzacji powyżej wartości z pkt 1.2 lp. 1.

3.5. Dokumentacja techniczna Systemu musi być dostępna w języku polskim lub angielskim; dokumentacja powykonawcza i materiały szkoleniowe – w języku polskim.

3.6. Wymagania sformułowane w rozdz. 4 słowem „musi” są wymaganiami obowiązkowymi – ich niespełnienie skutkuje odrzuceniem oferty. Wymagania sformułowane słowem „powinien” (pkt 49, 50, 52, 53, 54) są wymaganiami pożądanymi – ich niespełnienie nie skutkuje odrzuceniem oferty.

4. Wymagania funkcjonalne i techniczne Systemu

4.1. Wykonawca wypełni poniższą tabelę, wpisując w kolumnie „Spełnia” TAK lub NIE oraz podając w ostatniej kolumnie oferowane parametry lub sposób spełnienia wymagania (w tym, w miarę możliwości, odwołanie do dokumentacji producenta).

4.2. Wymagania dotyczące wartości liczbowych są wymaganiami minimalnymi; dopuszcza się parametry lepsze.

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
0	Producent, nazwa i wersja oferowanego oprogramowania NAC oraz nazwa/oznaczenie oferowanej licencji i licencji wsparcia technicznego producenta.	—	Producent: …… Nazwa i wersja: …… Licencje: ……
A. Podstawowa funkcjonalność systemu NAC			
1	System musi posiadać funkcjonalność aktywnego zapobiegania dostępowi do sieci nieautoryzowanych użytkowników i urządzeń końcowych.		
2	System musi współpracować z urządzeniami wielu producentów (tzw. multi-vendor).		
3	System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli; interfejs WEB w wersji HTML5 niewymagający obsługi dodatkowych wtyczek.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
4	System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.		
5	System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.		
6	System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.		
7	System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do co najmniej 200 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.		
8	Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.		
9	System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) w liczbie co najmniej równej liczbie licencji na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.		
10	System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: – VM – min. VMware ESXi co najmniej w wersji 5.x, Hyper-V w wersji min. 2012, Proxmox w wersji min. 5.x, KVM , Citrix XenServer w wersji min. 4.x, – maszyny fizyczne – serwery wspierane przez producenta.		
11	System musi posiadać funkcjonalność serwerów: – serwera RADIUS dla infrastruktury sieciowej, – serwera OTP dla infrastruktury VPN, Captive Portal, TACACS+, – serwera SYSLOG, – serwera TACACS+, – serwera monitoringu, – serwera DHCP, – serwera polityk uwierzytelniania i kontroli dostępu 802.1X, – serwera WWW (HTTP/HTTPS) dla uwierzytelniania gościnnego.		
12	System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
13	System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji, w tym OpenLDAP, Microsoft Active Directory, WebServices/API, RADIUS, relacyjnych baz danych: min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.		
14	System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji, w tym OpenLDAP, Microsoft Active Directory, Google G Suite, WebServices/API, RADIUS, relacyjnych baz danych: min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.		
15	System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, RADIUS, OpenLDAP, relacyjne bazy danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), Check Point, ServiceNow).		
16	Podczas synchronizacji system musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenie lokalnych haseł, certyfikatów oraz wysyłanie konfiguracji dostępowych poprzez e-mail.		
17	System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.		
18	System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także niepołączonymi relacjami zaufania.		
19	System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.		
20	System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.		
21	System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. login, hasło, imię, nazwisko, e-mail, status).		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
22	System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji i kasowania.		
23	Interfejs graficzny systemu musi być dostępny w różnych wersjach językowych (min. w języku polskim i angielskim).		
24	System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.		
25	System musi posiadać możliwość raportowania podłączonych tożsamości i urządzeń końcowych podłączonych do sieci, min.: tożsamość, adres MAC, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.		
26	System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny z podglądem wszystkich portów i modułów zarządzanego urządzenia.		
27	System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.		
28	System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.		
29	System musi posiadać funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu zmian konfiguracji oraz konfiguracji ustawień portu w zakresie min. VLAN-ów, autoryzacji, statusu, opisu.		
30	System musi obsługiwać automatyczne egzekwowanie zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.		
31	System musi posiadać możliwość konfiguracji serwera DHCP dla utworzonych podsieci IP.		
32	System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.		
33	System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach, minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
34	System musi posiadać funkcjonalność wysyłania zdarzeń, np. do systemów SIEM, minimum protokołem Syslog, z informacjami z serwerów autoryzacji, DHCP, VPN, OTP, TACACS+.		
35	System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.		
36	System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).		
37	System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google i LinkedIn.		
38	System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez e-mail, bramkę SMS oraz zapasową bramkę SMS.		
39	System musi posiadać funkcję personalizacji strony gościnnej.		
40	Captive Portal musi się automatycznie dostosowywać formatem do podłączonego urządzenia końcowego, min.: komputer, tablet, telefon.		
41	Captive Portal musi umożliwiać rejestrację gości potwierdzaną przez konta typu sponsor.		
42	Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego w Google Authenticator lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.		
43	Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.		
44	Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.		
45	Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.		
46	Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np. pole tekstowe, lista wyboru.		
47	Interfejs graficzny Captive Portalu musi być dostępny w różnych wersjach językowych (min. w języku polskim, angielskim, niemieckim, hiszpańskim, francuskim i ukraińskim).		
48	Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
49	Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie oraz okresowo, wg zadanej liczby dni.		
50	Captive Portal powinien umożliwiać konfigurację maksymalnej liczby nieudanych logowań.		
51	System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP i CDP.		
52	System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołów, min. Syslog, SNMP Trap, REST API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.		
53	System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością dodania tożsamości, urządzenia końcowego lub adresu MAC do kwarantanny.		
54	System powinien posiadać mechanizm rozłączania sesji min. przez SNMP, komendy CLI, RADIUS CoA zgodnie z RFC 5176.		
55	System musi posiadać dedykowanego agenta min. dla systemów Windows, macOS, Linux w celu profilowania urządzeń końcowych.		
56	System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia i systemu operacyjnego, co najmniej przez: DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, RADIUS, WMI, MDM, WinRM, ONVIF.		
57	System musi umożliwiać integrację z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).		
58	System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum dla systemów: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.		
59	System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa, co najmniej: – czy system jest aktualny – z możliwością automatycznego naprawienia niezgodności, – czy włączona jest zapora sieciowa (firewall),		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
	– czy uruchomiony jest system antywirusowy i czy baza sygnatur jest aktualna, – czy włączone jest szyfrowanie dysku systemowego, – czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory, – czy na dysku znajdują się pliki lub katalogi wskazane przez administratora, – czy w systemie są uruchomione procesy wskazane przez administratora, – czy w systemie są uruchomione usługi wskazane przez administratora – z możliwością automatycznego naprawienia niezgodności, – czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: • wartości klucza rejestru, • typu wartości: Number, String, Version.		
60	System musi posiadać możliwość wysyłania komunikatów do użytkowników min. za pomocą agenta i Captive Portalu.		
61	System musi współpracować z serwerem tokenów.		
62	System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT, co najmniej dla systemów: – Microsoft Windows, – macOS, – iOS, – Android.		
63	System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).		
64	System musi wspierać protokół IPv6 min. dla konsoli SSH, komunikacji RADIUS, NTP, SNMP oraz komunikacji z Microsoft Active Directory.		
B. Mechanizmy uwierzytelniania			
65	System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.		
66	System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: – MAC, – PAP/ASCII, – CHAP,		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
	– SNMP, – 802.1X, wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania, np. IEEE 802.1X (PEAP), IEEE 802.1X (EAP-TLS), IEEE 802.1X (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP itp.		
67	System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.		
68	System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.		
69	System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows 10, Windows 11, Apple macOS Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).		
70	System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: – tożsamość/urządzenie końcowe, – grupa tożsamości/urządzeń końcowych, – parametry urządzeń końcowych, min.: system operacyjny, wersja, – atrybuty Active Directory, – jednostka organizacyjna tożsamości/urządzeń końcowych, – urządzenia sieciowe sieci przewodowej i bezprzewodowej, – grupy urządzeń sieciowych, – porty urządzeń sieciowych, – grupy portów urządzeń sieciowych, – jednostka organizacyjna portów, – punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), – data, czas ważności polityki, – wewnętrzny Captive Portal, – metoda autoryzacji.		
71	System musi umożliwiać przypisywanie sieci VLAN i/lub zwrotnych atrybutów RADIUS VSA podczas etapu autoryzacji, np. ACL, Quality of Service, co najmniej dla następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MikroTik, Ubiquiti Networks.		
72	System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP i adresu MAC.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
73	System musi wspierać funkcjonalność autorejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego i adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.		
74	System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.		
75	System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.		
76	System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.		
77	System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.		
78	System musi umożliwiać tworzenie hasła dnia dla tożsamości zarejestrowanych przez wewnętrzny Captive Portal.		
79	System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.		
80	System musi wspierać uwierzytelnianie urządzeń końcowych na podstawie adresów MAC zawartych w lokalnej bazie.		
81	System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal WWW.		
82	System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.		
83	System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP, zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.		
C. Obsługa serwerów certyfikatów CA			

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
84	System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.		
85	Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać co najmniej następujące funkcjonalności: – możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych, – możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych, – możliwość generowania certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol), – usługę OCSP (Online Certificate Status Protocol).		
D. Obsługa serwerów DHCP			
86	System musi posiadać funkcję zintegrowanego serwera DHCP.		
87	System musi wspierać funkcjonalność autorejestracji, polegającą na łączeniu urządzenia końcowego i adresu MAC podczas pracy serwera DHCP.		
88	System musi zapewniać co najmniej następujące funkcjonalności serwera DHCP: – uruchamianie usługi dla wybranych podsieci, – przypisanie ustalonego adresu IP dla adresu MAC, – przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci, – możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC, – możliwość określania braku dostępu dla wybranych adresów MAC, – monitoring obciążenia pul dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC, – możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP, – możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego, – możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi, – dokonywanie zmian bez konieczności wyłączania usług.		
E. Obsługa serwerów TACACS+			

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu do urządzeń sieciowych, w tym:			
89	System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.		
90	System musi umożliwiać tworzenie haseł administratorom.		
91	System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.		
92	System musi raportować wszystkie wydane komendy na kontrolowanych urządzeniach sieciowych.		
93	System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.		
94	System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.		
95	System musi wspierać logowanie administratorów za pomocą tokenów OTP.		
96	System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.		
F. Raportowanie i monitoring			
System musi umożliwiać generowanie raportów oraz monitoring co najmniej następujących parametrów:			
97	Monitoring autoryzacji.		
98	Monitoring zdarzeń systemowych.		
99	Monitoring zdarzeń DHCP.		
100	Monitoring tożsamości.		
101	Monitoring urządzeń końcowych.		
102	Monitoring urządzeń sieciowych.		
103	Raport stanu systemu (min. szczegółowe dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostatnie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenie portów – przepustowość, liczba autoryzacji), dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu e-mail.		
104	Raport ze zdarzeń logowania z informacją o nadanym adresie IP.		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
105	Raport stanu systemu z poziomu konsoli CLI, min.: obciążenie procesora, pamięci, przestrzeni dyskowej, działanie usług.		
106	Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.		
107	System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.		
108	System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.		
109	System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLAN-ów w urządzeniach sieciowych działających w środowisku.		
110	System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.		
111	System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych, w tym: podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min.: system operacyjny, wersja.		
112	System musi umożliwiać podgląd tożsamości i urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych i kontrolerów Wi-Fi.		
113	Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji oraz o tokenach wysłanych przez bramkę SMS.		
114	Raport zdarzeń Microsoft Active Directory, minimum: – logowania i wylogowania z systemu, w tym błędne logowania, – logowania do sieci 802.1X.		
G. Alarmy i diagnostyka			
115	System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: – wiadomości e-mail, – Syslog, – notyfikacji systemowych.		
116	Alarmy muszą móc być generowane co najmniej w sytuacjach: – przekroczenia ilości obsługiwanych transakcji RADIUS,		

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)	Parametry oferowane / sposób spełnienia
	– opóźnienia obsługi transakcji RADIUS, – statusu krytycznego modułów.		
117	System musi posiadać zestaw narzędzi diagnostycznych do rozwiązywania problemów, w tym: – badanie łączności IP za pomocą ping, traceroute, – tcpdump protokołów RADIUS, TACACS+, – wyszukiwanie zdarzeń RADIUS z uwzględnieniem: • nazwy użytkownika, • adresu MAC, • statusu uwierzytelnienia (udane lub nieudane), • powodu, jeżeli uwierzytelnienie było nieudane, • zakresu czasowego, co do dnia, godziny i minuty, – wykonanie zdalnego polecenia na urządzeniu sieciowym.		

5. Wdrożenie Systemu

5.1. Analiza przedwdrożeniowa

- Wykonawca w terminie do 7 dni od zawarcia umowy przeprowadzi analizę środowiska (urządzenia sieciowe, segmentacja VLAN, Active Directory, rodzaje urządzeń końcowych, w tym urządzenia nieobsługujące 802.1X).
- Na jej podstawie Wykonawca opracuje projekt techniczny wdrożenia, obejmujący m.in. architekturę Systemu, politykę dostępu dla poszczególnych grup, plan etapowania i plan wycofania zmian. Projekt wymaga akceptacji Zamawiającego.

5.2. Instalacja

- Instalacja Systemu na infrastrukturze wirtualizacyjnej Zamawiającego, w tym konfiguracja instalacji rozproszonej / wysokiej dostępności i Disaster Recovery.
- Aktualizacja do najnowszej stabilnej wersji, zabezpieczenie konfiguracji (hardening), ograniczenie dostępu do panelu administracyjnego do segmentu zarządzania, konfiguracja kont administratorów i ról.
- Konfiguracja cyklicznej kopii bezpieczeństwa i przeprowadzenie testu odtworzenia.

5.3. Integracje

- Integracja z Microsoft Active Directory, przełącznikami i kontrolerem Wi-Fi/punktami dostępowymi wskazanymi w pkt 2.1 (RADIUS, RADIUS CoA, SNMP).
- Przekazywanie zdarzeń do systemu SIEM / serwera Syslog Zamawiającego.
- zaporą sieciową / VPN (OTP) i serwerem DHCP.

5.4. Polityki dostępu

- Pracownicy i komputery służbowe – uwierzytelnianie 802.1X (EAP-TLS z certyfikatami lub PEAP z przypisaniem VLAN/ACL.

- Urządzenia bez suplikanta 802.1X (drukarki, telefony VoIP, urządzenia IoT) – uwierzytelnianie MAC z profilowaniem urządzeń.
- Goście – Captive Portal z rejestracją potwierdzaną przez sponsora, osobny VLAN z dostępem wyłącznie do Internetu; BYOD – rejestracja urządzeń prywatnych.
- Agent i badanie zgodności (posture) dla komputerów służbowych, VLAN kwarantanny i komunikaty dla użytkowników.

5.5. Uruchomienie etapowe

- System zostanie najpierw uruchomiony w trybie monitorowania (bez blokowania dostępu) na okres nie krótszy niż 7 dni, w celu inwentaryzacji urządzeń i weryfikacji polityk.
- Włączanie egzekwowania polityk odbywać się będzie stopniowo (np. według przełączników lub segmentów), w oknach serwisowych uzgodnionych z Zamawiającym, z zachowaniem planu wycofania zmian.

5.6. Testy odbiorowe

- Testy obejmą co najmniej: dostęp pracownika (802.1X), dostęp urządzenia bez suplikanta (MAC), odmowę dostępu dla nieznanego urządzenia, przypisanie do VLAN kwarantanny dla urządzenia niezgodnego z polityką, rejestrację gościa przez Captive Portal, rozłączenie sesji (CoA), przekazanie zdarzeń do SIEM, odtworzenie z kopii bezpieczeństwa oraz procedurę awaryjną.
- Scenariusze testów Wykonawca przedstawi do akceptacji Zamawiającego przed ich przeprowadzeniem.

5.7. Dokumentacja powykonawcza

- Wykonawca przekaże w języku polskim dokumentację powykonawczą zawierającą m.in.: opis architektury i konfiguracji, polityki dostępu, konfigurację urządzeń sieciowych w zakresie NAC, procedury administracyjne, procedurę kopii bezpieczeństwa i odtwarzania oraz procedurę awaryjną (przywrócenie dostępu do sieci w przypadku niedostępności Systemu).
- Wykonawca przekaże Zamawiającemu wszystkie hasła i poświadczenia utworzone w trakcie wdrożenia.

5.8. Prace wykonywane będą w siedzibie Zamawiającego lub zdalnie, wyłącznie za pośrednictwem kanału dostępu wskazanego i kontrolowanego przez Zamawiającego. Osoby realizujące wdrożenie podpiszą zobowiązanie do zachowania poufności.

6. Szkolenie

6.1. Wykonawca przeprowadzi szkolenie w zakresie użytkowania i administrowania wdrożonym Systemem NAC dla **2 osób** wskazanych przez Zamawiającego.

6.2. Szkolenie odbędzie się w wymiarze **4 godzin zegarowych** (1 godzina = 60 minut), w jednym dniu roboczym, w godzinach 8:00–16:00. Czas przerw nie wlicza się do czasu szkolenia.

6.3. Szkolenie zostanie przeprowadzone w jednej z następujących form, **według wyboru Zamawiającego**:

- **stacjonarnej** – w siedzibie Zamawiającego; Zamawiający zapewni salę, a Wykonawca ponosi wszelkie koszty związane z dojazdem i pobytem prowadzącego;
- **zdalnej (online)** – w czasie rzeczywistym, z udziałem prowadzącego, z możliwością zadawania pytań i udostępniania ekranu, za pośrednictwem platformy zapewnionej przez Wykonawcę, niewymagającej zakupu licencji ani instalacji płatnego oprogramowania po stronie Zamawiającego. Zamawiający nie dopuszcza szkolenia w formie nagrania lub kursu e-learningowego.

6.4. Zamawiający poinformuje Wykonawcę o wybranej formie szkolenia przy uzgadnianiu terminu, nie później niż 3 dni robocze przed terminem szkolenia.

6.5. Szkolenie odbędzie się po zakończeniu wdrożenia Systemu i będzie uwzględniać konfigurację wdrożoną u Zamawiającego. Ćwiczenia praktyczne prowadzone będą na wdrożonym Systemie lub na środowisku testowym, w sposób niezakłócający pracy sieci produkcyjnej.

6.6. Szkolenie przeprowadzi osoba posiadająca praktyczną wiedzę w zakresie oferowanego Systemu (np. certyfikat producenta lub doświadczenie we wdrożeniach Systemu).

6.7. Ramowy program szkolenia (szczegółowy program Wykonawca przedstawi do akceptacji Zamawiającego nie później niż 3 dni roboczych przed terminem szkolenia):

Lp.	Zakres tematyczny	Czas (orientacyjnie)
1	Architektura i elementy wdrożonego Systemu, konsola zarządzania, konta i uprawnienia administratorów	30 min
2	Polityki uwierzytelniania i autoryzacji: 802.1X, uwierzytelnianie MAC, przypisywanie VLAN/ACL, kwarantanna, rozłączanie sesji (CoA)	60 min
3	Obsługa gości i BYOD: Captive Portal, konta sponsorskie, autokonfiguratory sieci, certyfikaty (CA)	30 min
4	Profilowanie urządzeń, agent i badanie zgodności (posture)	30 min
5	Monitoring, raporty, alarmy, przekazywanie zdarzeń do SIEM	30 min
6	Utrzymanie Systemu: kopie bezpieczeństwa i odtwarzanie, aktualizacje, narzędzia diagnostyczne, procedura awaryjna	30 min
7	Pytania uczestników, podsumowanie	30 min
	Razem	**240 min**

6.8. Wykonawca dostarczy każdemu uczestnikowi materiały szkoleniowe w języku polskim w postaci elektronicznej, najpóźniej w dniu szkolenia. Zamawiający może je wykorzystywać na potrzeby własne bez ograniczeń czasowych.

6.9. Po zakończeniu szkolenia uczestnicy otrzymają imienne zaświadczenia potwierdzające uczestnictwo w szkoleniu oraz nabycie umiejętności obsługi Systemu NAC.

6.10. Szczegółowy plan i termin szkolenia zostaną uzgodnione przez Wykonawcę z Zamawiającym. Potwierdzeniem realizacji szkolenia będzie lista obecności (w formie zdalnej – raport uczestnictwa z platformy) oraz protokół odbioru szkolenia.

7. Licencja wsparcia technicznego producenta

7.1. Wykonawca dostarczy wraz z dożywotnią licencją Systemu NAC 12-miesięczną licencję na wsparcie producenta oprogramowania, liczoną od dnia podpisania protokołu odbioru końcowego. Licencja ta musi obejmować co najmniej:

- kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą Systemu NAC,
- rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem, a także wsparcie przy identyfikacji problemów trudnych do powtórzenia,
- wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów konfiguracji oprogramowania, a także wstępne obejścia dla wykrytych problemów,

- dostęp do dokumentacji i instrukcji na stronie internetowej,
- dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

7.2. Zgłoszenia mogą być składane w języku polskim lub angielskim.

8. Termin realizacji i odbiór

8.1. Termin realizacji zamówienia do 14 dni od zawarcia umowy.

8.2. Szkolenie: do 14 dni od dnia zawarcia umowy, w terminie uzgodnionym z Zamawiającym.

8.3. Odbiór realizowany będzie protokołami: odbioru dostawy licencji, odbioru wdrożenia (po pozytywnych testach z pkt 5.6), odbioru szkolenia oraz protokołem odbioru końcowego. Zamawiający może odmówić odbioru w przypadku stwierdzenia niezgodności z OPZ.

9. Rozwiązania równoważne

9.1. Wskazane w OPZ nazwy systemów, produktów i producentów (np. Microsoft Active Directory, Microsoft Intune, FortiGate, Cisco) określają systemy i urządzenia, z którymi oferowany System musi współpracować, i nie stanowią wskazania przedmiotu zamówienia.

9.2. Jeżeli w OPZ wskazano znak towarowy, patent, pochodzenie lub normę w odniesieniu do przedmiotu zamówienia, Zamawiający dopuszcza rozwiązania równoważne, zapewniające co najmniej parametry i funkcjonalności opisane w OPZ (art. 99 ust. 5 i 6 ustawy Pzp). Wykazanie równoważności spoczywa na Wykonawcy.

9.3. Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne”.

9.4. Wymienione w jakiejkolwiek części OPZ nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

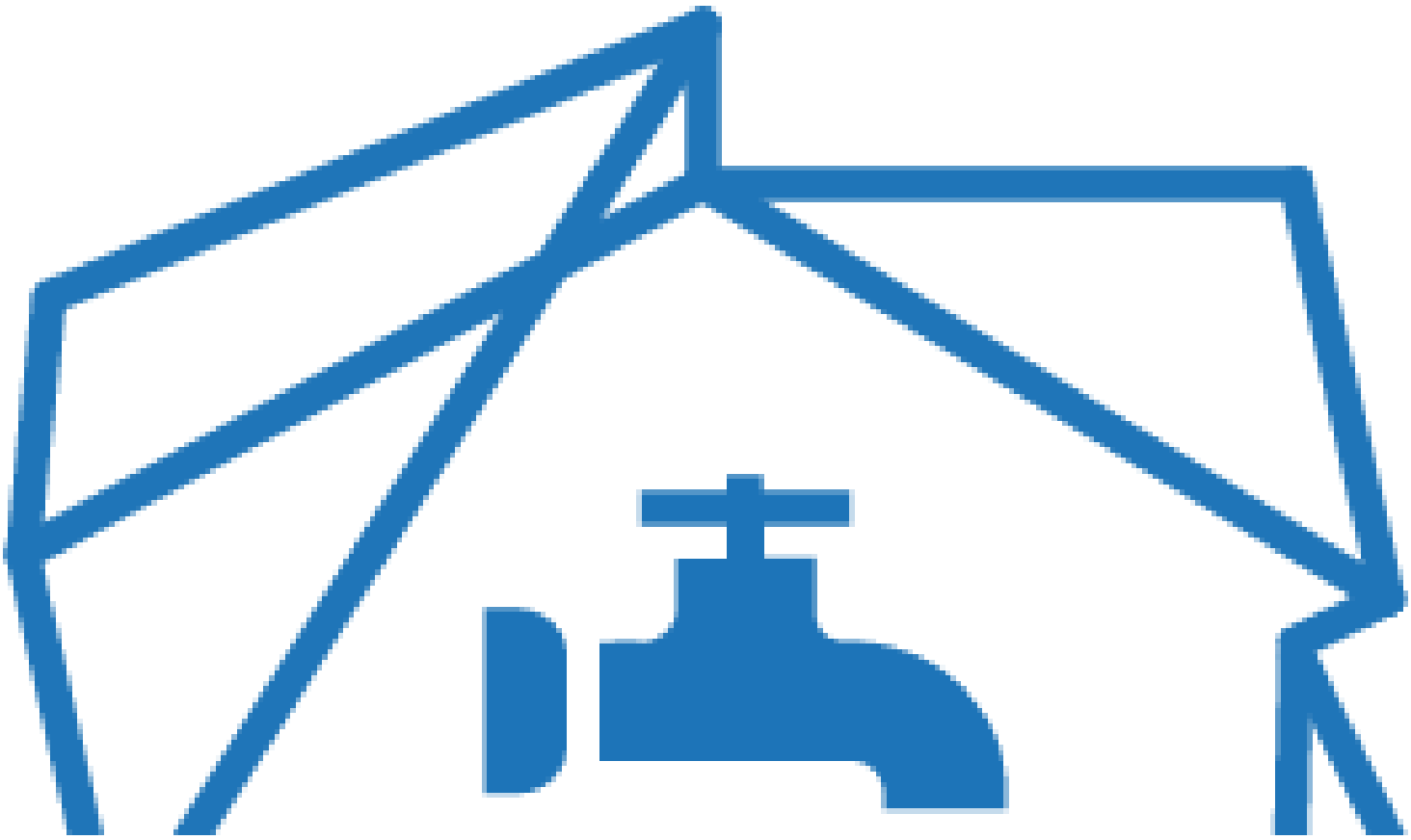
9.5. Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy Zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny".

9.6. Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,

- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

9.7. Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.



OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu wykrywania i reagowania na zagrożenia sieciowe (NDR) wraz z platformą sprzętową i przełącznikiem sieciowym zarządzalnym w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa i wdrożenie dwóch niezależnych, fabrycznie nowych systemów klasy NDR (Network Detection and Response) przeznaczonych do wykrywania i automatycznego reagowania na zagrożenia w sieci IT oraz w sieci OT Zamawiającego, w szczególności ruch boczny (lateral movement), skanowanie portów oraz aktywność oprogramowania ransomware.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Oprogramowanie NDR (licencja) – zgodnie z pkt 1–5 tabeli w rozdz. 3	2 kpl. (1 – sieć IT, 1 – sieć OT)
2.	Platforma sprzętowa NDR (serwer sieciowy) wraz z dyskami SSD – zgodnie z pkt 6–12 tabeli w rozdz. 3	2 szt. (1 – sieć IT, 1 – sieć OT)
3.	Dyski twarde HDD – zgodnie z pkt 11 tabeli w rozdz. 3	2 szt. na każdą platformę (łącznie min. 4 szt.)
4.	Przełącznik sieciowy zarządzalny – zgodnie z pkt 13–16 tabeli w rozdz. 3	2 szt. (1 – sieć IT, 1 – sieć OT)
5.	Usługa wdrożenia systemu NDR w dwóch niezależnych sieciach IT i OT – zgodnie z rozdz. 4	1 usługa

1.3. Oferowane oprogramowanie NDR, platforma sprzętowa, dyski oraz przełącznik muszą stanowić spójne, w pełni współpracujące ze sobą rozwiązanie. W szczególności przełącznik musi być obsługiwany przez oferowane oprogramowanie NDR w zakresie przekazywania pakietów do analizy (pkt 1 i 16 tabeli) oraz automatycznej izolacji hostów na poziomie portu (pkt 4 tabeli), a dyski muszą być obsługiwane przez oferowaną platformę sprzętową.

1.4. Zamówienie obejmuje dostawę dwóch kompletnych zestawów (oprogramowanie NDR, platforma sprzętowa z dyskami, przełącznik) oraz ich wdrożenie: jednego zestawu w sieci IT i jednego zestawu w sieci OT Zamawiającego, zgodnie z rozdz. 4. Zestawy muszą działać jako dwa całkowicie niezależne systemy.

1.5. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 48820000-2 Serwery; 32420000-3 Urządzenia sieciowe; 30233132-5 Napędy dysków twardych; 51612000-5 Usługi instalowania sprzętu do przetwarzania informacji; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Dostarczony sprzęt musi być fabrycznie nowy, nieużywany, nierefabrykowany, nieeksponowany na wystawach, wyprodukowany nie wcześniej niż 12 miesięcy przed dniem dostawy i pochodzić z oficjalnego kanału dystrybucji producenta na rynek Unii Europejskiej.

2.2. Sprzęt musi posiadać oznakowanie CE oraz deklarację zgodności UE, a także spełniać wymagania dyrektywy RoHS.

2.3. Licencja na oprogramowanie NDR musi być udzielona na czas nieoznaczony (bezterminowo), bez ograniczeń czasowych działania funkcji wymienionych w tabeli w rozdz. 3 i bez konieczności ponoszenia przez Zamawiającego opłat cyklicznych. Licencja musi być wystawiona na Zamawiającego.

2.4. Wykonawca zapewni dostęp do aktualizacji oprogramowania NDR (w tym reguł i mechanizmów detekcji) oraz oprogramowania układowego (firmware) platformy i przełącznika przez okres nie krótszy niż okres gwarancji, bez dodatkowych opłat.

2.5. Dyski twarde muszą znajdować się na liście kompatybilności producenta oferowanej platformy sprzętowej, a przełącznik – na liście urządzeń obsługiwanych przez oferowane oprogramowanie NDR (jeżeli producent publikuje takie listy).

2.6. Interfejs zarządzania oprogramowania NDR, platformy sprzętowej i przełącznika musi być dostępny w języku polskim lub angielskim.

2.7. Wynik procesora w teście CPU Mark (pkt 6 tabeli) Zamawiający będzie weryfikował według stanu na stronie https://www.cpubenchmark.net/ na dzień publikacji ogłoszenia. Wykonawca dołączy do oferty wydruk wyniku z tej strony.

2.8. Wraz ze sprzętem Wykonawca dostarczy komplet elementów niezbędnych do jego uruchomienia i montażu, w tym kable zasilające, szyny lub zestawy do montażu w szafie rack 19” oraz dokumentację użytkownika w języku polskim lub angielskim (dopuszcza się wersję elektroniczną).

3. Szczegółowe wymagania techniczne

Oferowane rozwiązanie musi spełniać co najmniej poniższe wymagania minimalne. Wykonawca wypełnia kolumnę „Dane oferowanego produktu / spełnienie wymagań minimalnych”.

Lp.	Parametr	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Dane oferowanego produktu / spełnienie wymagań minimalnych
Wymagania funkcjonalne dla oprogramowania NDR			
	Producent, nazwa i wersja oprogramowania	Należy podać	……
1.	Analiza pakietów	System musi realizować analizę selektywną dedykowanych pakietów sieciowych przekazywanych z przełączników (np. poprzez technologię mirroring/SPAN lub dedykowane API sterujące).	spełnia/nie spełnia *)
2.	Model wdrażania	System musi działać jako dedykowana, samodzielna aplikacja/instancja (typu Standalone) instalowana bezpośrednio na posiadanej lub dostarczonej platformie serwerowej pamięci masowej (NAS) bez konieczności dokupowania cyklicznych licencji oprogramowania (model licencjonowania wieczystego lub wbudowanego w ekosystem sprzętowy).	spełnia/nie spełnia *)
3.	Analiza behawioralna oparta na sztucznej inteligencji (AI)	System musi wykorzystywać algorytmy uczenia maszynowego i sztucznej inteligencji do stałego monitorowania anomalii w ruchu sieciowym w celu wykrywania ataków typu lateral movement (ruch boczny), skanowania portów oraz infekcji ransomware wewnątrz sieci.	spełnia/nie spełnia *)

Lp.	Parametr	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Dane oferowanego produktu / spełnienie wymagań minimalnych
4.	Automatyczna izolacja (Auto-isolation)	W przypadku wykrycia krytycznego zagrożenia (np. aktywności ransomware) system musi posiadać funkcję automatycznego wydania instrukcji do przełącznika sieciowego w celu natychmiastowego odcięcia/odizolowania zainfekowanego hosta na poziomie portu.	spełnia/nie spełnia *)
5.	Scentralizowany panel	Zarządzanie systemem musi odbywać się poprzez responsywny, graficzny interfejs webowy (GUI) umożliwiający szybką weryfikację wektorów ataków oraz topologii sieciowej.	spełnia/nie spełnia *)
Platforma sprzętowa NDR (serwer sieciowy)			
	Producent i model	Należy podać	……
6.	Procesor	Architektura x86, minimum 4-rdzeniowy, 4-wątkowy procesor osiągający co najmniej 5000 pkt w teście CPU Mark – https://www.cpubenchmark.net/	spełnia/nie spełnia *) wynik: …… pkt
7.	Pamięć operacyjna	Minimum 16 GB pamięci RAM typu DDR5, zainstalowanej w dostarczonym urządzeniu.	spełnia/nie spełnia *)
8.	Zatoki na dyski (HDD)	Minimum 4 zatoki formatu 3,5 cala SATA 6 Gb/s z pełnym wsparciem dla technologii Hot-swap (wymiana dysków w trakcie pracy systemu) oraz natywną kompatybilnością z nośnikami 2,5 cala.	spełnia/nie spełnia *)
9.	Interfejsy M.2 (SSD)	Minimum 3 gniazda na dyski M.2 2280 PCIe, w tym minimum 2 obsadzone dyskami SSD NVMe o pojemności minimum 500 GB każdy, przeznaczonymi na bazę danych i logi systemu NDR (konfiguracja RAID 1).	spełnia/nie spełnia *) producent/model dysku SSD: ……
10.	Interfejsy sieciowe	Minimum 2 wbudowane porty miedziane RJ45 o przepustowości minimum 2,5 GbE każdy, wspierające automatyczną negocjację prędkości (2,5G/1G/100M).	spełnia/nie spełnia *)
11.	Dyski twarde (HDD)	Minimum 2 sztuki dysków twardych HDD klasy Enterprise lub dedykowanych do systemów NAS pracujących w trybie całodobowym 24/7/365 (np. seria WD Red Pro, Seagate IronWolf Pro lub równoważne). Pojemność pojedynczego dysku: minimum 4 TB.	spełnia/nie spełnia *) producent/model dysku: ……
12.	Obudowa	Typu RACK 1U z szynami do montażu w szafie RACK.	spełnia/nie spełnia *)
Przełącznik sieciowy zarządzalny			
	Producent i model	Należy podać	……
13.	Porty miedziane high-speed	Minimum 4 porty 10GbE RJ45 Multi-Gigabit (pełne wsparcie i dopasowanie do prędkości 10G/5G/2.5G/1G/100M).	spełnia/nie spełnia *)

Lp.	Parametr	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Dane oferowanego produktu / spełnienie wymagań minimalnych
14.	Porty światłowodowe	Minimum 8 portów 10GbE SFP+ dedykowanych dla szybkich połączeń szkieletowych i uplink (obsługa modułów SFP+ oraz kabli bezpośredniego połączenia DAC).	spełnia/nie spełnia *)
15.	Zarządzanie i funkcje L2	Zarządzanie przez przeglądarkę Web (interfejs graficzny), pełna obsługa standardów: VLAN (802.1Q), agregacja łączy (LACP), IGMP Snooping, mechanizmy zapobiegania pętlom (STP/RSTP). Dedykowany port 1GbE RJ45 do zarządzania przełącznikiem.	spełnia/nie spełnia *)
16.	Przechwytywanie ruchu (SPAN)	Pełna i natywna obsługa funkcji Port Mirroring (SPAN) oraz selektywnego kopiowania ruchu (np. mirroring na podstawie reguł ACL) – zdolność kopiowania ruchu wejściowego i wyjściowego z wybranych portów/VLAN-ów, w zakresie wymaganym przez oferowane oprogramowanie NDR, i przesyłania go na dedykowany fizyczny port analityczny spięty z serwerem NDR.	spełnia/nie spełnia *)

*) niepotrzebne skreślić. Niespełnienie któregokolwiek z wymagań minimalnych skutkuje odrzuceniem oferty jako niezgodnej z warunkami zamówienia.

4. Wdrożenie w sieciach IT i OT

4.1. Zasady ogólne

4.1.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży jeden kompletny zestaw, obejmujący oprogramowanie NDR, platformę sprzętową z dyskami i przełącznik.

4.1.2. Zestawy dla sieci IT i OT muszą działać całkowicie niezależnie. Zamawiający nie dopuszcza wspólnej konsoli zarządzania, wspólnych kont administracyjnych, synchronizacji konfiguracji ani danych ani jakichkolwiek połączeń sieciowych między zestawami. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych ani podłączać do sieci OT urządzeń, które wcześniej pracowały w sieci IT, bez zgody Zamawiającego.

4.1.3. Interfejsy zarządzania platformy, oprogramowania NDR i przełącznika w każdej sieci muszą być dostępne wyłącznie z wydzielonego segmentu (VLAN) zarządzania danej sieci, wskazanego przez Zamawiającego.

4.1.4. Jeżeli sieć OT nie ma dostępu do Internetu, Wykonawca skonfiguruje zestaw OT do pracy bez połączenia z chmurą producenta i przekaże procedurę aktualizacji w trybie offline (z nośnika lub przez wskazany przez Zamawiającego serwer pośredniczący).

4.1.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym.

4.2. Analiza przedwdrożeniowa i projekt techniczny

4.2.1. W terminie do 7 dni od zawarcia umowy Wykonawca przeprowadzi, wspólnie z Zamawiającym, analizę przedwdrożeniową każdej sieci, obejmującą co najmniej: segmenty i sieci VLAN objęte

monitorowaniem, punkty włączenia przełącznika NDR w istniejącą infrastrukturę, adresację, segment zarządzania oraz listę urządzeń krytycznych.

4.2.2. Na podstawie analizy Wykonawca opracuje odrębny projekt techniczny wdrożenia dla sieci IT i dla sieci OT, zawierający schemat połączeń, adresację, konfigurację przełącznika, zakres przekazywania ruchu do analizy, polityki reagowania oraz harmonogram prac. Prace instalacyjne mogą rozpocząć się po akceptacji projektu przez Zamawiającego.

4.3. Zakres prac w każdej sieci

- montaż platformy sprzętowej i przełącznika w szafie rack wskazanej przez Zamawiającego, podłączenie zasilania (w tym do zasilania gwarantowanego UPS, jeżeli jest dostępne) i okablowania krosowego oraz trwałe oznakowanie urządzeń i przewodów;
- instalacja dysków, konfiguracja macierzy RAID 1 dla dysków HDD oraz dla dysków SSD przeznaczonych na bazę danych i logi systemu NDR;
- aktualizacja systemu operacyjnego platformy, oprogramowania NDR i oprogramowania układowego przełącznika do najnowszych wersji udostępnionych przez producenta;
- utwardzenie konfiguracji (hardening): zmiana wszystkich domyślnych haseł, wyłączenie zbędnych usług i protokołów, dostęp administracyjny wyłącznie przez HTTPS/SSH z segmentu zarządzania, imienne konta administratorów z podziałem uprawnień, uwierzytelnianie wieloskładnikowe (jeżeli jest obsługiwane), synchronizacja czasu z serwerem NTP wskazanym przez Zamawiającego;
- konfiguracja przełącznika: sieci VLAN, port analityczny, przekazywanie ruchu do analizy (SPAN lub mirroring selektywny), integracja z oprogramowaniem NDR w zakresie izolacji portów oraz włączenie przełącznika w istniejącą infrastrukturę sieciową zgodnie z projektem;
- instalacja i konfiguracja oprogramowania NDR: rejestracja przełącznika, inwentaryzacja wykrytych urządzeń, konfiguracja mechanizmów wabików (honeypot/threat trap) – jeżeli rozwiązanie je udostępnia, polityk ochrony, list wyjątków oraz powiadomień (e-mail i syslog do systemu wskazanego przez Zamawiającego, np. SIEM);
- wykonanie kopii zapasowej konfiguracji wszystkich urządzeń po zakończeniu wdrożenia i przekazanie jej Zamawiającemu.

4.4. Polityki reagowania

4.4.1. Po uruchomieniu systemu w każdej sieci Wykonawca przeprowadzi okres obserwacji i strojenia reguł trwający nie krócej niż 7 dni, w celu ograniczenia fałszywych alarmów. Automatyczną izolację można włączyć dopiero po zakończeniu tego okresu.

4.4.2. Sieć IT: system będzie automatycznie izolował hosty, dla których wykryto zagrożenia o wysokim lub krytycznym poziomie ryzyka. Urządzenia infrastrukturalne wskazane przez Zamawiającego (np. serwery, kontrolery domeny, urządzenia sieciowe) zostaną objęte listą wyjątków lub trybem wymagającym potwierdzenia administratora.

4.4.3. Sieć OT: domyślnie system będzie pracował w trybie monitorowania i powiadamiania, bez automatycznej izolacji. Automatyczną izolację można włączyć wyłącznie dla urządzeń wskazanych przez Zamawiającego na piśmie. Urządzenia sterowania procesem (m.in. sterowniki PLC, RTU, serwery SCADA, stacje HMI) muszą zostać wyłączone z automatycznej izolacji.

4.4.4. W obu sieciach administrator musi mieć możliwość ręcznego cofnięcia izolacji z poziomu konsoli NDR.

4.5. Testy odbiorowe

Wykonawca przeprowadzi w każdej sieci testy według scenariusza zaakceptowanego przez Zamawiającego, z użyciem własnego hosta testowego i nieszkodliwych narzędzi (bez użycia rzeczywistego złośliwego oprogramowania). Testy obejmą co najmniej:

- potwierdzenie poprawnego przekazywania ruchu z przełącznika do analizy;

- wykrycie symulowanego skanowania portów z hosta testowego;
- wykrycie symulowanej próby ruchu bocznego (np. prób logowania SMB/SSH do innego hosta lub wabika);
- w sieci IT – automatyczną izolację hosta testowego na poziomie portu przełącznika i jej ręczne cofnięcie;
- w sieci OT – wygenerowanie alertu bez izolacji hosta oraz ręczną izolację i cofnięcie izolacji hosta testowego;
- dostarczenie powiadomień e-mail i komunikatów syslog do wskazanego systemu;
- brak dostępu do interfejsów zarządzania spoza segmentu zarządzania oraz brak połączeń między zestawami IT i OT.

4.6. Dokumentacja i instruktaż

4.6.1. Wykonawca przekaże w języku polskim odrębną dokumentację powykonawczą dla sieci IT i dla sieci OT, obejmującą co najmniej: schemat połączeń, adresację, wyeksportowane konfiguracje urządzeń, wykaz kont, opis polityk reagowania i list wyjątków, protokoły z testów oraz procedury: obsługi alertu, cofnięcia izolacji, aktualizacji (dla sieci OT – również w trybie offline), wymiany dysku oraz odtworzenia konfiguracji. Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

4.6.2. Wykonawca przeprowadzi w siedzibie Zamawiającego instruktaż dla administratorów w wymiarze nie mniejszym niż **4** godzin dla maksymalnie **2** osób, obejmujący obsługę obu zestawów, analizę zdarzeń, zarządzanie politykami i izolacją oraz procedury z pkt 4.6.1.

4.6.3. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT.

5. Gwarancja i serwis

5.1. Wykonawca udzieli gwarancji na cały przedmiot zamówienia, w tym na prawidłowe działanie wykonanej konfiguracji, na okres nie krótszy niż **24** miesięcy, liczony od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń.

5.2. Gwarancja musi być realizowana przez producenta lub autoryzowanego partnera serwisowego producenta na terenie Polski. Zgłoszenia przyjmowane są w dni robocze, telefonicznie, e-mailem lub przez portal serwisowy.

5.3. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych. Czas naprawy lub wymiany urządzenia na wolne od wad: nie dłuższy niż **3** dni roboczych od zgłoszenia. Po wymianie urządzenia Wykonawca odtworzy jego konfigurację.

5.4. Uszkodzone nośniki danych (dyski HDD oraz SSD) pozostają u Zamawiającego i nie podlegają zwrotowi do Wykonawcy ani producenta, bez utraty uprawnień gwarancyjnych.

5.5. Koszty transportu sprzętu w ramach gwarancji ponosi Wykonawca.

6. Termin, miejsce realizacji i odbiór

6.1. Termin realizacji zamówienia do **14** dni od dnia zawarcia umowy.

6.2. Miejsce realizacji: Siedziba Zamawiającego. Dostawa odbywa się na koszt i ryzyko Wykonawcy, w dni robocze w godzinach **8:00-16:00**, po wcześniejszym uzgodnieniu terminu z Zamawiającym.

6.3. Odbiór dostawy nastąpi na podstawie protokołu odbioru ilościowo-jakościowego, po sprawdzeniu kompletności dostawy i zgodności z ofertą. Wraz z dostawą Wykonawca przekaże dokumenty licencyjne oraz dokumenty gwarancyjne.

6.4. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 4.5 oraz przekazaniu dokumentacji z pkt 4.6.1. Po odbiorze wdrożenia w obu sieciach i przeprowadzeniu instruktażu strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazane w opisie przedmiotu zamówienia nazwy własne, znaki towarowe, normy lub pochodzenie (w tym przykładowe serie dysków w pkt 11 tabeli) mają charakter przykładowy i służą wyłącznie określeniu wymaganego standardu jakościowego i funkcjonalnego. Zamawiający dopuszcza rozwiązania równoważne.

7.2. Za rozwiązanie równoważne Zamawiający uzna rozwiązanie o parametrach technicznych, funkcjonalnych i jakościowych nie gorszych niż wymagane w niniejszym OPZ. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.

7.3. Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne”.

7.4. Wymienione w jakiejkolwiek części OPZ nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

7.5. Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy Zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny".

7.6. Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

7.7. Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu zarządzania dostępem uprzywilejowanym (PAM) wraz z serwisem producenta oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji na system klasy PAM (Privileged Access Management), służący do ochrony kont uprzywilejowanych i kluczy SSH, pośredniczenia w dostępie uprzywilejowanym, monitorowania i rejestrowania sesji uprzywilejowanych oraz raportowania wykorzystania kont uprzywilejowanych, dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wraz z serwisem producenta oraz usługą wdrożenia.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencja bezterminowa na system PAM dla co najmniej 5 użytkowników – zgodnie z rozdz. 2 i 3	2 kpl. (1 – sieć IT, 1 – sieć OT) na 24 miesięcy
2.	Serwis (wsparcie producenta i dystrybutora, aktualizacje) dla obu instancji (IT i OT) – zgodnie z rozdz. 4	24 miesięcy
3.	Usługa wdrożenia systemu PAM w dwóch niezależnych sieciach IT i OT, wraz z instruktażem administratorów	1 usługa

1.3. Zamówienie obejmuje dostawę licencji dla dwóch instancji systemu PAM: jednej przeznaczonej dla sieci IT i jednej dla sieci OT Zamawiającego. Instancje muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.5 i rozdz. 5. Wymagania z rozdz. 3 dotyczą każdej z instancji.

1.4. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 72268000-1 Usługi dostawy oprogramowania; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być wystawione na Zamawiającego, obejmować zakres określony w pkt 7–9 tabeli w rozdz. 3 i zostać udzielone na okres 24 miesięcy od dnia podpisania protokołu odbioru licencji. Liczba użytkowników: co najmniej 5 dla instancji IT i co najmniej 5 dla instancji OT.

2.2. Wygaśnięcie licencji terminowej nie może powodować utraty dostępu Zamawiającego do poświadczeń zapisanych w sejfie, nagrań sesji ani logów zdarzeń – Zamawiający musi mieć możliwość ich odczytu i eksportu.

2.3. System musi być instalowany w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Hyper-V lub VMware (pkt 3 tabeli), odrębnym dla sieci IT i dla sieci OT. Działanie funkcji systemu, w tym aktywacja licencji, nie może wymagać połączenia z chmurą producenta. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji w trybie offline.

2.4. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe (procesor, pamięć RAM, przestrzeń dyskowa, w tym na nagrania sesji przez okres **24** miesięcy) odrębnie dla instancji IT i OT, z uwzględnieniem klastra active-active z arbitrem (pkt 5–6 tabeli).

2.5. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własnym sejfem poświadczeń, bazą danych, kontami użytkowników, konfiguracją i

licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami. Klaster active-active (pkt 5 tabeli) może być zestawiony wyłącznie w ramach jednej sieci. Pośrednik (pkt 18–19 tabeli) instancji IT nie może być umieszczony w sieci OT, i odwrotnie.

2.6. System musi być dostarczony w najnowszej wersji dostępnej na dzień dostawy. Interfejs użytkownika i dokumentacja muszą być dostępne w języku polskim lub angielskim.

2.7. Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację serwisu u producenta na rzecz Zamawiającego, z uwzględnieniem wymagania z pkt 49 tabeli.

3. Wymagania funkcjonalne systemu PAM

Oferowany system musi spełniać co najmniej poniższe wymagania minimalne, odrębnie w każdej z instancji (IT i OT). Wykonawca wypełnia kolumnę „Spełnienie wymagań minimalnych".

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
	Producent, nazwa i wersja oferowanego systemu PAM	……
A. Ogólne – architektura		
1.	System PAM musi być rozwiązaniem bezagentowym, tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy, bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja.	spełnia/nie spełnia *)
2.	System musi umożliwiać uwierzytelnianie wieloskładnikowe i obsługiwać wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego, w tym co najmniej: routerów, przełączników, zapór sieciowych, a także aplikacji, baz danych itp.	spełnia/nie spełnia *)
3.	System musi być dostarczany w formie zamkniętej platformy wirtualnej, przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware. Przez zamkniętą platformę Zamawiający rozumie wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.	spełnia/nie spełnia *)
4.	Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobnych maszyn wirtualnych lub fizycznych. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej.	spełnia/nie spełnia *)
5.	Rozwiązanie musi oferować możliwość wdrożenia drugiej instancji i konfiguracji klastra typu active-active.	spełnia/nie spełnia *)
6.	Rozwiązanie musi posiadać możliwość wdrożenia komponentu zarządzającego klastrem w postaci arbitra.	spełnia/nie spełnia *)
B. Licencjonowanie		
7.	System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z systemu PAM (w każdej z instancji – IT i OT), obejmującym co najmniej następujące funkcjonalności: – ochronę kont uprzywilejowanych, – ochronę kluczy SSH, – zarządzanie i monitorowanie sesji uprzywilejowanych, – rejestrowanie sesji uprzywilejowanych, – raportowanie wykorzystania kont uprzywilejowanych.	spełnia/nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
8.	Dostarczone licencje na system PAM do ochrony kont uprzywilejowanych zostaną udzielone na okres 24 miesięcy (licencje terminowe).	spełnia/nie spełnia *)
9.	Dostarczone licencje na system PAM nie mogą w żaden sposób limitować liczby chronionych systemów docelowych.	spełnia/nie spełnia *)
10.	System powinien być dostarczony wraz z serwisem na okres 24 miesięcy, umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.	spełnia/nie spełnia *)
11.	W ramach zakupionych licencji użytkownicy systemu muszą mieć możliwość skorzystania z mechanizmu prywatnego sejfu do przechowywania haseł, notatek, plików itp.	spełnia/nie spełnia *)
12.	W ramach zakupionej licencji rozwiązanie powinno umożliwiać korzystanie z dodatkowych modułów: – modułu pozwalającego na automatyczne wyszukiwanie urządzeń w sieci, – modułu pozwalającego na tworzenie automatycznych zadań wykonywanych na zarządzanych urządzeniach, – modułu pozwalającego na zarządzanie rozwiązaniem za pomocą API.	spełnia/nie spełnia *)
C. Funkcjonalności		
Zarządzanie kontami i dostęp do systemów docelowych		
13.	System PAM musi zapewniać możliwość zarządzania co najmniej: – użytkownikami w systemach operacyjnych Windows, Unix/Linux, – kontami domenowymi Microsoft Active Directory, – kontami lokalnymi VMware ESX/ESXi, – kontami na urządzeniach, m.in.: Cisco, Aruba, Alcatel, Check Point, FortiGate, Huawei, IBM AIX, Brocade, – kontami baz danych: Microsoft SQL Server, Oracle, MySQL, PostgreSQL, – kontami do zarządzania i monitorowania serwerów, m.in. iLO, iDRAC, – kontami aplikacji webowych: Facebook, Google, Twitter (X), LinkedIn, Instagram, OpenStack, AWS, – kontami w innych, niewymienionych systemach i urządzeniach, do których dostęp odbywa się za pomocą protokołów: SSH, RDP, VNC, Telnet, HTTP/HTTPS, X11, – kluczami SSH.	spełnia/nie spełnia *)
14.	System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji.	spełnia/nie spełnia *)
15.	System PAM musi zapewniać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje i obsługując co najmniej następujące protokoły: SSH, RDP, VNC, Telnet, HTTP/HTTPS, X11.	spełnia/nie spełnia *)
16.	System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS, Sybase, Windows RM, Windows RPC, Windows SMB.	spełnia/nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
17.	System PAM musi umożliwiać dostęp użytkowników do systemu docelowego za pomocą następujących narzędzi: – przeglądarki internetowej, – klienta RDP, – klienta protokołu SSH/Telnet (np. PuTTY), – klienta serwerów bazodanowych, w tym co najmniej DBeaver.	spełnia/nie spełnia *)
18.	System PAM musi umożliwiać wykorzystanie pośrednika w komunikacji pomiędzy systemem PAM a systemem docelowym.	spełnia/nie spełnia *)
19.	Pośrednik musi być dostępny jako obraz dla usługi konteneryzacji Docker.	spełnia/nie spełnia *)
Uwierzytelnianie		
20.	System PAM musi wspierać co najmniej następujące mechanizmy uwierzytelniania: LDAP, RADIUS, TACACS+, Active Directory, OpenID, SAML.	spełnia/nie spełnia *)
21.	System PAM musi zapewniać możliwość uwierzytelniania dwuskładnikowego.	spełnia/nie spełnia *)
22.	System PAM musi wspierać integrację z rozwiązaniami uwierzytelniania dwuskładnikowego, takimi jak Google Authenticator i Microsoft Authenticator.	spełnia/nie spełnia *)
23.	System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego do różnych systemów, poprzez wiele kont uprzywilejowanych lub jedno konto.	spełnia/nie spełnia *)
Polityki dostępu		
24.	System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd haseł uprzywilejowanych.	spełnia/nie spełnia *)
25.	System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.	spełnia/nie spełnia *)
26.	System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszających: – możliwość rozpoczęcia sesji, – możliwość podglądu hasła, – podanie powodu rozpoczęcia sesji, – podanie powodu podglądu hasła, – możliwość rozpoczęcia sesji bez akceptacji w przypadku awarii, – możliwość podglądu hasła bez akceptacji w przypadku awarii, – konieczność akceptacji rozpoczęcia sesji przez innego administratora (administratorów), – konieczność akceptacji podglądu hasła przez innego administratora (administratorów), – akceptację na kilku poziomach, – dostęp do urządzeń i poświadczeń docelowych określonego typu, producenta, lokalizacji, – zakres godzin, dni oraz dat, w których użytkownik systemu będzie miał dostęp do poświadczeń.	spełnia/nie spełnia *)
27.	System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru czasu trwania takiego dostępu.	spełnia/nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
28.	System PAM musi oferować możliwość wykorzystania kont uprzywilejowanych niezapisanych w samym systemie – kont prywatnych użytkowników.	spełnia/nie spełnia *)
Logi i raportowanie		
29.	System PAM musi posiadać log wszystkich zdarzeń systemowych.	spełnia/nie spełnia *)
30.	System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji lub serwera.	spełnia/nie spełnia *)
31.	System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.	spełnia/nie spełnia *)
32.	System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.	spełnia/nie spełnia *)
33.	System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.	spełnia/nie spełnia *)
34.	Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.	spełnia/nie spełnia *)
35.	System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.	spełnia/nie spełnia *)
Zarządzanie hasłami		
36.	System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką, m.in.: – umożliwiać zdefiniowanie wymagań dotyczących długości hasła i znaków w haśle (małe i duże litery, cyfry, znaki specjalne), – automatycznie generować hasła kont systemów docelowych w sposób pseudolosowy, – generować unikalne hasła dla kont systemów docelowych, – wymuszać automatyczną zmianę hasła po jego podglądzie.	spełnia/nie spełnia *)
37.	System PAM musi umożliwiać przezroczyste (transparentne) połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.	spełnia/nie spełnia *)
Zarządzanie sesjami i nagrania		
38.	System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym.	spełnia/nie spełnia *)
39.	System PAM musi umożliwiać przerwanie lub zawieszenie trwającej sesji.	spełnia/nie spełnia *)
40.	System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sesji oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.	spełnia/nie spełnia *)
41.	System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).	spełnia/nie spełnia *)
42.	Audyt poleceń musi umożliwiać podjęcie co najmniej akcji „zablokuj polecenie” i „rozłącz sesję” po wykryciu audytowanego polecenia, a także automatyczne umieszczenie na liście zablokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.	spełnia/nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
43.	Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.	spełnia/nie spełnia *)
44.	System PAM musi umożliwiać konfigurację parametrów nagrań, w tym: – liczby klatek na sekundę, – jakości pojedynczej klatki, – formatu pojedynczej klatki: JPG lub PNG, – okresu przechowywania nagrań.	spełnia/nie spełnia *)
45.	System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika, co najmniej dla sesji SSH i RDP, oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.	spełnia/nie spełnia *)
46.	System PAM musi umożliwiać wyświetlenie w nagraniu sesji momentów aktywności ekranowej oraz wprowadzania danych z klawiatury przez użytkownika.	spełnia/nie spełnia *)
47.	System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o: – politykę dostępową, – urządzenie docelowe, – poświadczenie, – adres źródłowy.	spełnia/nie spełnia *)
48.	System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji.	spełnia/nie spełnia *)
Pozostałe		
49.	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, że zaoferowany produkt posiada wsparcie producenta na terenie Polski.	spełnia/nie spełnia *)
50.	System PAM musi być kompletny i pozwalać na uruchomienie co najmniej następujących funkcjonalności: – zarządzanie kontami uprzywilejowanymi w ramach organizacji, – monitorowanie wykorzystania kont uprzywilejowanych, – nagrywanie i archiwizowanie sesji zdalnych, – zagwarantowanie skalowalności rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług.	spełnia/nie spełnia *)
51.	System PAM musi umożliwiać personalizację wyglądu aplikacji, co najmniej poprzez umieszczenie logo Zamawiającego w głównym oknie aplikacji.	spełnia/nie spełnia *)

*) niepotrzebne skreślić. Niespełnienie któregokolwiek z wymagań minimalnych skutkuje odrzuceniem oferty jako niezgodnej z warunkami zamówienia. Wymagania sformułowane jako „powinien” / „powinno” mają charakter pożądany i nie stanowią podstawy odrzucenia oferty.

4. Serwis producenta

4.1. Wykonawca zapewni serwis producenta systemu PAM dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji, obejmujący wsparcie producenta oraz dystrybutora i pobieranie aktualizacji przygotowanych przez producenta (pkt 10 tabeli).

4.2. W ramach serwisu Zamawiający otrzyma co najmniej dostęp do nowych wersji i aktualizacji oprogramowania, w tym poprawek bezpieczeństwa platformy wirtualnej, dostęp do bazy wiedzy i dokumentacji producenta oraz możliwość zgłaszania problemów. Dla instancji OT producent powinien udostępniać aktualizacje w postaci pakietów do instalacji w trybie offline.

4.3. Zgłoszenia przyjmowane są przez portal producenta lub dystrybutora, e-mailem lub telefonicznie, w języku polskim lub angielskim. Czas reakcji na zgłoszenie: nie dłuższy niż **16** godzin roboczych; dla zgłoszeń krytycznych (niedostępność systemu lub sejfu poświadczeń) – nie dłuższy niż **8** godzin.

5. Wdrożenie w sieciach IT i OT

5.1. Zasady wdrożenia w sieciach IT i OT

5.1.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję systemu PAM, zgodnie z pkt 2.5.

5.1.2. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

5.1.3. Instancja IT obejmie wyłącznie systemy docelowe w sieci IT, a instancja OT – wyłącznie systemy docelowe w sieci OT. Dostęp użytkowników do instancji OT będzie możliwy wyłącznie z wyznaczonego segmentu sieci OT (np. strefy zdemilitaryzowanej OT lub stanowisk inżynierskich).

5.1.4. W sieci OT Wykonawca zastosuje bezpieczną konfigurację, w szczególności:

- automatyczna zmiana haseł (pkt 36 tabeli) oraz poświadczenia typu JIT (pkt 14 tabeli) na stacjach HMI, serwerach SCADA, stacjach inżynierskich i urządzeniach sterowania zostaną włączone wyłącznie dla kont wskazanych przez Zamawiającego, po weryfikacji zależności (usługi, aplikacje, połączenia między systemami) i potwierdzeniu zgodności z zaleceniami dostawców systemów sterowania; dla pozostałych kont hasła będą wyłącznie przechowywane w sejfie, a ich zmiana będzie wykonywana ręcznie w oknach serwisowych;
- moduł automatycznego wyszukiwania urządzeń i moduł zadań automatycznych (pkt 12 tabeli) będą uruchamiane wyłącznie dla systemów wskazanych przez Zamawiającego i w uzgodnionych oknach serwisowych; aktywne skanowanie sterowników PLC i RTU jest niedopuszczalne;
- dostęp użytkowników zewnętrznych (pkt 15 tabeli) do systemów OT będzie wymagał akceptacji upoważnionej osoby Zamawiającego dla każdej sesji (pkt 26 tabeli), ograniczenia czasowego i rejestrowania sesji, a podgląd sesji w czasie rzeczywistym (pkt 38 tabeli) będzie dostępny dla dyżurnego operatora;
- zostanie skonfigurowany i przetestowany dostęp w przypadku awarii (pkt 26 lit. e–f tabeli) oraz procedura dostępu do systemów sterowania w przypadku niedostępności systemu PAM, w tym przechowywanie kopii poświadczeń awaryjnych w zabezpieczonej formie offline (np. zaplombowana koperta w sejfie fizycznym);
- audyt poleceń (pkt 41–42 tabeli) zostanie uruchomiony w pierwszej kolejności w trybie wyłącznie rejestrowania, a akcje blokowania poleceń, rozłączania sesji i automatycznego blokowania użytkowników – po akceptacji Zamawiającego;
- zostanie uzgodniona z Zamawiającym procedura użycia funkcji zawieszenia wszystkich sesji i zablokowania dostępu (pkt 40 tabeli).

5.1.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób

niepowodujący przerw ani zakłóceń w procesie technologicznym. Objęcie zarządzaniem systemów w sieci OT poprzedzi instalacja pilotażowa na wskazanym przez Zamawiającego, ograniczonym zakresie systemów.

5.2. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

5.2.1. Opracowanie harmonogramu wdrożenia systemu w obu sieciach.

5.2.2. Przeprowadzenie analizy przedwdrożeniowej (inwentaryzacja kont uprzywilejowanych, systemów docelowych, zależności i procesów dostępu) oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

5.2.3. Instalacja i konfiguracja każdej z instancji w klastrze active-active z arbitrem (pkt 5–6 tabeli) w tym: utwardzenie konfiguracji (zmiana domyślnych haseł, ograniczenie dostępu do interfejsów zarządzania), konfiguracja kopii zapasowych, integracja z usługą katalogową, jeśli występuje, uruchomienie uwierzytelniania dwuskładnikowego (pkt 21 tabeli), przekazywanie logów do systemu SIEM właściwego dla danej sieci oraz umieszczenie logo Zamawiającego. Dla instancji OT – konfiguracja pracy bez dostępu do Internetu.

5.2.4. Objęcie zarządzaniem systemów docelowych wskazanych przez Zamawiającego, w tym konfiguracja polityk dostępu, akceptacji, zakresów czasowych, rejestrowania sesji i parametrów nagrań (pkt 44 tabeli) oraz – w zakresie uzgodnionym z Zamawiającym – zmiany haseł.

5.2.5. Konfiguracja ról i grup dostępu, raportów i dostępu do raportów, zgodnie z macierzą uprawnień uzgodnioną z Zamawiającym na etapie analizy przedwdrożeniowej.

5.2.6. Przygotowanie i przeprowadzenie scenariuszy testowych w każdej z sieci. Proponowane scenariusze zostaną przedłożone Zamawiającemu do akceptacji i muszą obejmować co najmniej:

- zestawienie sesji przez proxy dla każdego typu systemu docelowego i każdego narzędzia dostępu, rejestrację, odtworzenie i pobranie nagrania (pkt 48 tabeli) oraz zablokowanie polecenia z czarnej listy;
- akceptację dostępu z podaniem powodu, dostęp w określonym zakresie czasu oraz dostęp w przypadku awarii;
- zmianę hasła dla każdego typu systemu objętego zmianą haseł, w tym automatyczną zmianę po podglądzie;
- przełączenie awaryjne węzłów klastra oraz odtworzenie systemu z kopii zapasowej;
- dla instancji OT – aktualizację w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu oraz brak połączeń między instancjami IT i OT.

5.2.7. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej opis architektury i konfiguracji, wykaz systemów docelowych i kont objętych zarządzaniem, macierz uprawnień i polityk dostępu, protokoły z testów oraz procedury administracyjne (aktualizacja – dla sieci OT również w trybie offline, kopia zapasowa i odtworzenie, dostęp awaryjny). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

5.2.8. Przeprowadzenie instruktażu stanowiskowego dla administratorów Zamawiającego (co najmniej 2 osób, w wymiarze co najmniej 4 godzin), odrębnie dla instancji IT i OT, obejmującego obsługę i administrowanie systemem, procedury dostępu awaryjnego, odtwarzania z kopii zapasowej i aktualizacji w trybie offline.

5.2.9. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT. Wykonawca nie może zachować kopii poświadczeń uzyskanych w trakcie wdrożenia; po zakończeniu prac hasła kont użytych przez

Wykonawcę zostaną zmienione. Jeżeli Wykonawca będzie miał dostęp do danych osobowych (np. w nagraniach sesji), strony zawrą umowę powierzenia przetwarzania danych osobowych.

5.2.10. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

6. Terminy realizacji i odbiór

6.1. Termin realizacji zamówienia do **14** dni od dnia podpisania umowy.

6.2. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji oraz potwierdzenia rejestracji serwisu producenta.

6.3. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 5.2.6, przekazaniu dokumentacji z pkt 5.2.7 i przeprowadzeniu instruktażu z pkt 5.2.8. Po odbiorze wdrożenia w obu sieciach strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazanie w OPZ nazw systemów, urządzeń, aplikacji i narzędzi, z którymi oferowany system musi współpracować (m.in. Hyper-V, VMware ESX/ESXi, Microsoft Windows, Microsoft Active Directory, Cisco, Aruba, Alcatel, Check Point, FortiGate, Huawei, IBM AIX, Brocade, Microsoft SQL Server, Oracle, MySQL, PostgreSQL, iLO, iDRAC, Facebook, Google, Twitter (X), LinkedIn, Instagram, OpenStack, AWS, Cassandra, Elasticsearch, MongoDB, Redis, Solr, Sybase, PuTTY, DBeaver, Docker, Google Authenticator, Microsoft Authenticator), wynika z infrastruktury i narzędzi wykorzystywanych przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

7.2. Pozostałe nazwy własne, znaki towarowe lub normy wskazane w OPZ mają charakter przykładowy. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.

7.3. Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne”.

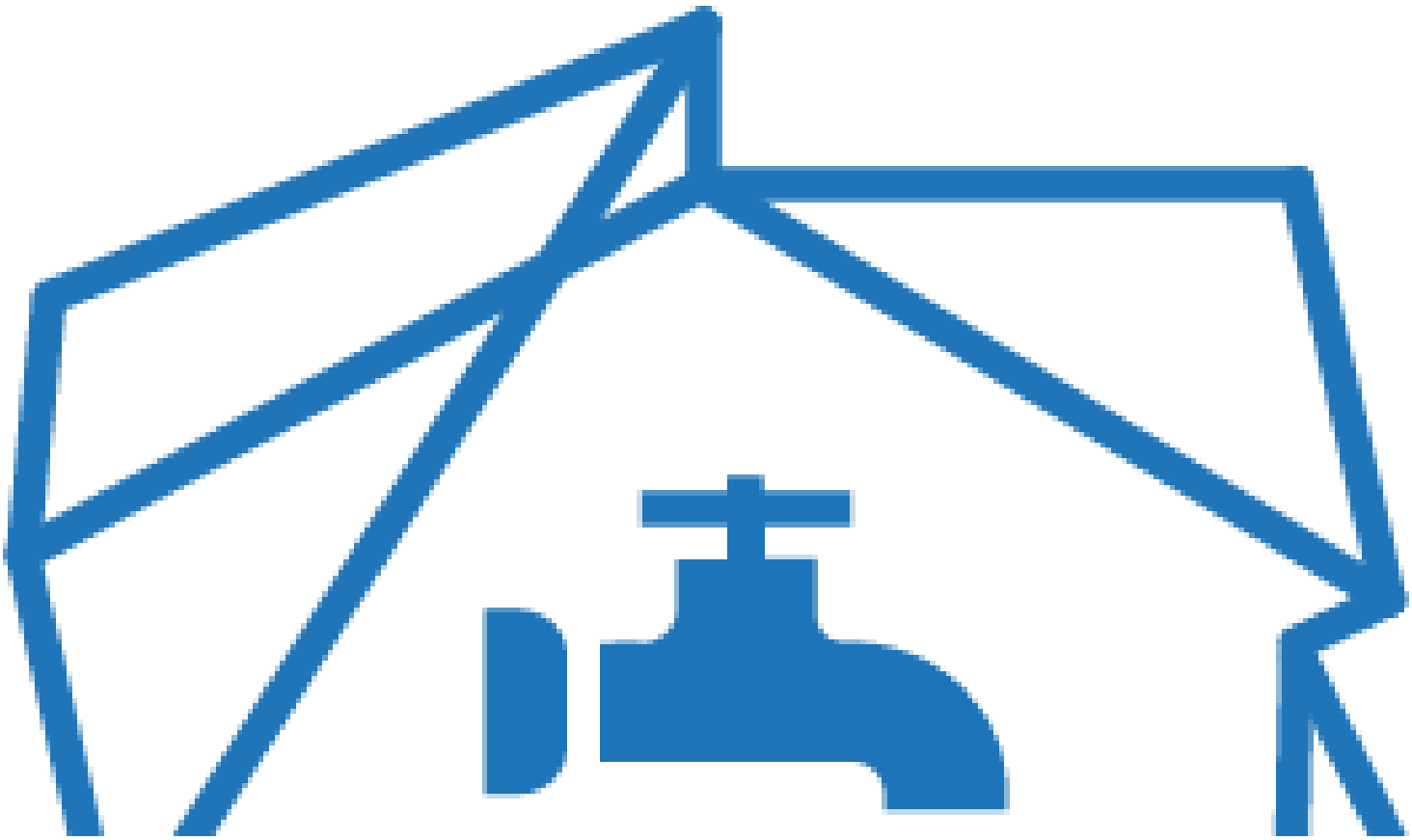
7.4. Wymienione w jakiejkolwiek części OPZ nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

7.5. Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy Zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny".

7.6. Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

7.7. Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.



OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu do zarządzania infrastrukturą IT (inwentaryzacja sprzętu i oprogramowania, zarządzanie oprogramowaniem i audyt legalności, automatyzacja zarządzania, powiadomienia i alerty) wraz ze wsparciem producenta oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji bezterminowych na oprogramowanie do kompleksowego zarządzania infrastrukturą IT (dalej: „System"), obejmujące inwentaryzację sprzętu i oprogramowania, zarządzanie oprogramowaniem i audyt legalności oprogramowania, automatyzacje zarządzania, powiadomienia i alerty, dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wraz ze wsparciem producenta oraz usługą wdrożenia.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencje bezterminowe na System – instancja dla sieci IT, w zakresie funkcjonalności z sekcji A–P tabeli w rozdz. 3	**50** stanowisk (agentów) **1** licencji konsoli administracyjnej
2.	Licencje bezterminowe na System – instancja dla sieci OT, w zakresie funkcjonalności z sekcji A–C, F, H, I, L–P tabeli w rozdz. 3	**20** stanowisk (agentów) **1** licencji konsoli administracyjnej
3.	Wsparcie producenta (asysta serwisowa) dla obu instancji – zgodnie z rozdz. 4	24 miesiące
4.	Usługa wdrożenia Systemu w dwóch niezależnych sieciach IT i OT wraz z instruktażem administratorów	1 usługa

1.3. Instancje dla sieci IT i OT muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.8 i rozdz. 5. Wymagania z rozdz. 3 dotyczą każdej z instancji w zakresie sekcji wskazanych dla niej w pkt 1.2.

1.4. Kod CPV: 48780000-4 Pakiety oprogramowania do zarządzania systemem, pamięcią i treścią; 48900000-7 Różne pakiety oprogramowania i systemy komputerowe; 72268000-1 Usługi dostawy oprogramowania; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być licencjami bezterminowymi (udzielonymi na czas nieoznaczony), wystawionymi na Zamawiającego, obejmującymi liczbę stanowisk (agentów) oraz licencji konsoli administracyjnej wskazaną w pkt 1.2. Licencje nie mogą ograniczać liczby użytkowników Systemu, zasobów ewidencjonowanych bez agenta.

2.2. Po zakończeniu okresu wsparcia producenta każda z instancji musi nadal działać w pełnym zakresie funkcjonalnym, z wykorzystaniem ostatniej zainstalowanej wersji oprogramowania, bez konieczności ponoszenia dodatkowych opłat.

2.3. System musi być instalowany w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Zamawiającego, odrębnym dla sieci IT i dla sieci OT. Działanie Systemu, w tym aktywacja licencji, nie może wymagać stałego połączenia z usługami chmurowymi producenta. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji oprogramowania i bazy wzorców oprogramowania w trybie offline.

2.4. Funkcje wykorzystujące zewnętrzne usługi chmurowe (w szczególności funkcje AI, integracja z usługą modelu językowego, chmurowe skanowanie plików, geolokalizacja) muszą być domyślnie wyłączone lub możliwe do całkowitego wyłączenia przez administratora, tak aby żadne dane nie były przekazywane poza infrastrukturę Zamawiającego bez jego decyzji.

2.5. Funkcje monitorowania aktywności użytkowników (w szczególności z sekcji C i D tabeli w rozdz. 3) muszą być konfigurowalne niezależnie dla poszczególnych grup komputerów i użytkowników oraz możliwe do wyłączenia, w celu dostosowania zakresu monitorowania do regulaminu pracy i przepisów prawa pracy obowiązujących u Zamawiającego.

2.6. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe i systemowe (procesor, pamięć RAM, przestrzeń dyskowa, system operacyjny, silnik bazy danych) niezbędne do działania każdej z instancji dla liczby stanowisk wskazanej w pkt 1.2.

2.7. Oprogramowanie musi być dostarczone w najnowszej wersji dostępnej na dzień dostawy. Interfejs użytkownika (konsola administracyjna) musi być dostępny w języku polskim. Dokumentacja i pomoc kontekstowa muszą być dostępne w języku polskim (dopuszcza się wersję elektroniczną). Licencje i wsparcie muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej; Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację wsparcia na rzecz Zamawiającego.

2.8. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własnym serwerem aplikacji, bazą danych, kontami użytkowników, konfiguracją i licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami.

3. Wymagania funkcjonalne Systemu

Oferowane oprogramowanie musi zapewniać co najmniej poniższe funkcjonalności, odrębnie w każdej z instancji (IT i OT), w zakresie sekcji wskazanych dla danej instancji w pkt 1.2. Wykonawca wypełnia kolumnę „Spełnienie wymagań minimalnych”.

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
	Producent, nazwa i wersja oferowanego oprogramowania	……
A. Zarządzanie zasobami (sprzęt i wyposażenie)		
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne		
1.	Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania	spełnia / nie spełnia *)
2.	Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP, SNMP oraz WMI	spełnia / nie spełnia *)
3.	Identyfikacja systemów Windows i Linux na podstawie skanu sieciowego	spełnia / nie spełnia *)
4.	Automatyczne wykrywanie interfejsów sieciowych, ich typów oraz adresów IP, MAC, DNS, systemu operacyjnego wraz z informacją o aktualizacji	spełnia / nie spełnia *)
5.	Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy	spełnia / nie spełnia *)
6.	Odwzorowanie struktury organizacji w oparciu o Active Directory	spełnia / nie spełnia *)
7.	Jednostronna synchronizacja komputerów oraz drukarek z AD, Entra ID oraz Intune (odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)	spełnia / nie spełnia *)
8.	Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz Entra ID) oraz sieci	spełnia / nie spełnia *)
9.	Mapowanie atrybutów obiektów AD (oraz Entra ID) do obiektów systemowych	spełnia / nie spełnia *)
10.	Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)	spełnia / nie spełnia *)
11.	Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
12.	Utworzenie własnych typów elementów wyposażenia	spełnia / nie spełnia *)
13.	Łączenie elementów wyposażenia w zestawy	spełnia / nie spełnia *)
14.	Przypisywanie zasobu do wielu zestawów	spełnia / nie spełnia *)
15.	Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia	spełnia / nie spełnia *)
16.	Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach	spełnia / nie spełnia *)
17.	Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików	spełnia / nie spełnia *)
18.	Przypisywanie sprzętu do konkretnych osób	spełnia / nie spełnia *)
19.	Przypisywanie sprzętu do wybranej firmy	spełnia / nie spełnia *)
20.	Automatyczne wyznaczanie „głównego użytkownika” komputera	spełnia / nie spełnia *)
21.	Wiązanie wielu rekordów wyposażenia z użytkownikiem	spełnia / nie spełnia *)
22.	Przypisywanie sprzętu do dowolnej lokalizacji	spełnia / nie spełnia *)
23.	Definiowanie własnych, dowolnych atrybutów sprzętu	spełnia / nie spełnia *)
24.	Przydzielanie aktywnym komputerom (bez określonego statusu) statusu „W użyciu”	spełnia / nie spełnia *)
25.	Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia	spełnia / nie spełnia *)
26.	Dowolna treść kodu kreskowego	spełnia / nie spełnia *)
27.	Określanie loga firmy oraz użycia go na wydrukach	spełnia / nie spełnia *)
28.	Grupowa zmiana domeny/grupy roboczej zasobu	spełnia / nie spełnia *)
29.	Możliwość łączenia zasobów w zestawy na podstawie typu oraz atrybutów zasobu	spełnia / nie spełnia *)
Informacje o sprzęcie		
30.	Automatyczne wykrywanie typu komputera (Desktop/Notebook/Serwer/kontroler domeny) na podstawie wyników skanowania sprzętu	spełnia / nie spełnia *)
31.	Wykrywanie komputerów typu All-In-One	spełnia / nie spełnia *)
32.	Automatyczne wykrywanie typów stacji roboczej (Tower/Desktop/SFF/uSFF)	spełnia / nie spełnia *)
33.	Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu	spełnia / nie spełnia *)
34.	Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM	spełnia / nie spełnia *)
35.	Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany	spełnia / nie spełnia *)
36.	Definiowanie statusów dla sprzętu (nowy, do kasacji, w serwisie itd.)	spełnia / nie spełnia *)
37.	Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)	spełnia / nie spełnia *)
38.	Odczyt informacji o module TPM	spełnia / nie spełnia *)
39.	Odczyt D3Dscore z WinSAT	spełnia / nie spełnia *)
40.	Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: switch, router, access point, bridge, modem, NAS, UPS itd.)	spełnia / nie spełnia *)
41.	Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu	spełnia / nie spełnia *)
42.	Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)	spełnia / nie spełnia *)
43.	Automatyczne tworzenie zestawów: komputer + monitor	spełnia / nie spełnia *)
44.	Automatyczne utworzenie zestawów: komputer + drukarka lokalna	spełnia / nie spełnia *)
45.	Automatyczne utworzenie zestawów: host + maszyny wirtualne	spełnia / nie spełnia *)
46.	Automatyczne wykrywanie czy komputer jest maszyną wirtualną	spełnia / nie spełnia *)
47.	Wykrywanie maszyn wirtualnych typu Parallels Virtual Platform	spełnia / nie spełnia *)
48.	Określanie informacji o wykorzystywanej wirtualizacji	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
49.	Podgląd zestawów, do których należy zasób	spełnia / nie spełnia *)
50.	Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami	spełnia / nie spełnia *)
51.	Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu	spełnia / nie spełnia *)
52.	Definiowanie szczegółowych informacji finansowych	spełnia / nie spełnia *)
53.	Obsługa walut w danych finansowych	spełnia / nie spełnia *)
54.	Definiowanie bazy dostawców sprzętu i oprogramowania	spełnia / nie spełnia *)
55.	Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)	spełnia / nie spełnia *)
56.	Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta	spełnia / nie spełnia *)
57.	Odczyt przez agenta identyfikator SID komputera	spełnia / nie spełnia *)
58.	Określanie adresu interfejsu webowego urządzenia sieciowego	spełnia / nie spełnia *)
59.	Określanie typu gwarancji dla zasobu	spełnia / nie spełnia *)
60.	Określenie wpływu biznesowego wybranego zasobu	spełnia / nie spełnia *)
61.	Tworzenie własnych typów gwarancji	spełnia / nie spełnia *)
62.	Określanie ikony dla typów zasobów	spełnia / nie spełnia *)
63.	Integracja z API producenta sprzętu, co najmniej Dell	spełnia / nie spełnia *)
64.	Wyszukiwanie i identyfikacja duplikatów zasobów	spełnia / nie spełnia *)
65.	Geolokalizacja komputerów z agentem	spełnia / nie spełnia *)
Raporty zasobów		
66.	Raport dodanych załączników	spełnia / nie spełnia *)
67.	Automatyczne tworzenie historii zmian sprzętu	spełnia / nie spełnia *)
68.	Raport zbiorczy historii zmian w sprzęcie	spełnia / nie spełnia *)
69.	Ewidencja zdarzeń serwisowych	spełnia / nie spełnia *)
70.	Dodawanie notatek/komentarzy dla zdefiniowanych obiektów zasobów	spełnia / nie spełnia *)
71.	Informacja na temat pojemności dysków twardych oraz wolnego miejsca	spełnia / nie spełnia *)
72.	Wydruk/dodawanie jako załącznik protokołu przekazania/zwrotu/utylizacji sprzętu	spełnia / nie spełnia *)
73.	Wydruk/dodawanie jako załącznik protokołu przekazania dla całego zestawu	spełnia / nie spełnia *)
74.	Kreator szablonów wydruków WYSIWYG	spełnia / nie spełnia *)
75.	Definiowanie dedykowanych profili protokołów	spełnia / nie spełnia *)
76.	Generowanie protokołów szyfrowania komputerów / telefonów	spełnia / nie spełnia *)
77.	Zapisywanie protokołów podczas generowania jako załącznik do zasobu	spełnia / nie spełnia *)
78.	Wydruk/dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia	spełnia / nie spełnia *)
79.	Wydruk lub zapis do pliku raportów ze szczegółami sprzętu	spełnia / nie spełnia *)
80.	Porównywarka wyników skanowania sprzętu	spełnia / nie spełnia *)
81.	Dzienniki zdarzeń systemu Windows	spełnia / nie spełnia *)
82.	Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu	spełnia / nie spełnia *)
Zarządzanie zasilaniem		
83.	Zdalne włączanie i wyłączenie komputerów	spełnia / nie spełnia *)
84.	Obsługa SecureOn przy Wake-on-LAN	spełnia / nie spełnia *)
85.	Tworzenie harmonogramów wyłączania i włączania komputerów	spełnia / nie spełnia *)
86.	Wybór trybu zamknięcia systemu, co najmniej: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart	spełnia / nie spełnia *)
87.	Możliwość anulowania /wyświetlenia komunikatu, jeśli jest zalogowany użytkownik	spełnia / nie spełnia *)
88.	Możliwość przerwania / odłożenia zadania na żądanie użytkownika	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
89.	Wymuszenie wylogowania użytkownika przed wyłączeniem komputera	spełnia / nie spełnia *)
90.	Raport zadań jednorazowych oraz harmonogramów	spełnia / nie spełnia *)
91.	Monitoring obciążenia CPU	spełnia / nie spełnia *)
Funkcje dodatkowe		
92.	Zdalne wykonywanie skryptów (batch/PowerShell) – Obsługa zadań jednorazowych i cyklicznych	spełnia / nie spełnia *)
93.	Generowanie skryptów z wykorzystaniem AI	spełnia / nie spełnia *)
94.	Podpisywanie skryptów PowerShell certyfikatem	spełnia / nie spełnia *)
95.	Wykonywanie skryptów w kontekście sesji użytkownika lub usługi	spełnia / nie spełnia *)
96.	Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika	spełnia / nie spełnia *)
97.	Wykonywanie zadań dla wszystkich komputerów	spełnia / nie spełnia *)
98.	Edytor skryptów z funkcją kolorowania składni	spełnia / nie spełnia *)
99.	Wykorzystywanie predefiniowanych skryptów	spełnia / nie spełnia *)
100.	Import informacji o wyposażeniu z pliku CSV	spełnia / nie spełnia *)
101.	Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta sprzętu, co najmniej Dell	spełnia / nie spełnia *)
102.	Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)	spełnia / nie spełnia *)
103.	Generowanie kodów kreskowych i QR dla każdego elementu wyposażenia	spełnia / nie spełnia *)
104.	Obsługa kodów QR	spełnia / nie spełnia *)
105.	Archiwum zasobów	spełnia / nie spełnia *)
106.	Przeniesienie utylizowanego wyposażenia do archiwum	spełnia / nie spełnia *)
107.	Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego	spełnia / nie spełnia *)
108.	Powiadomienia o kończącej się gwarancji/umowie serwisowej dla zasobu	spełnia / nie spełnia *)
109.	Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych	spełnia / nie spełnia *)
110.	Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej	spełnia / nie spełnia *)
111.	Grupowa zmiana atrybutów	spełnia / nie spełnia *)
112.	Personalizacja statusów zasobów	spełnia / nie spełnia *)
B. Zarządzanie oprogramowaniem		
Licencje		
128.	Inwentaryzacja licencji	spełnia / nie spełnia *)
129.	Automatyczne tworzenie licencji na podstawie kluczy produktów	spełnia / nie spełnia *)
130.	Odczyt klucza OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego	spełnia / nie spełnia *)
131.	Import licencji z pliku tekstowego	spełnia / nie spełnia *)
132.	Automatyczne generowanie historii zmian w licencji	spełnia / nie spełnia *)
133.	Określanie statusu licencji	spełnia / nie spełnia *)
134.	Tworzenie własnych atrybutów licencji	spełnia / nie spełnia *)
135.	Tworzenie notatek oraz załączników w dowolnym formacie do licencji	spełnia / nie spełnia *)
136.	Tworzenie licencji z poziomu rozliczenia audytu legalności	spełnia / nie spełnia *)
137.	Tworzenie licencji z poziomu raportu kluczy licencji	spełnia / nie spełnia *)
138.	Tworzenie zestawów licencji	spełnia / nie spełnia *)
139.	Relacja licencji z użytkownikiem, firmą, działem, lokalizacją	spełnia / nie spełnia *)
140.	Zmiana typu licencji dla wybranej grupy	spełnia / nie spełnia *)
141.	Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
142.	Przypisywanie licencji do komputera	spełnia / nie spełnia *)
143.	Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)	spełnia / nie spełnia *)
144.	Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska	spełnia / nie spełnia *)
145.	Definiowanie licencji przeznaczonych do przyszłego zakupu	spełnia / nie spełnia *)
146.	Definiowanie kluczy seryjnych i przypisywanie do licencji	spełnia / nie spełnia *)
147.	Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją	spełnia / nie spełnia *)
148.	Określenie wpływu biznesowego wybranej licencji	spełnia / nie spełnia *)
Skanowanie oprogramowania		
149.	Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera	spełnia / nie spełnia *)
150.	Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów	spełnia / nie spełnia *)
151.	Śledzenie zmian w stanie zainstalowanego oprogramowania	spełnia / nie spełnia *)
152.	Zdalny skan komputerów (bieżący lub okresowy)	spełnia / nie spełnia *)
153.	Zmiana priorytetu skanowania oprogramowania	spełnia / nie spełnia *)
154.	Skan komputerów niepodłączonych do sieci	spełnia / nie spełnia *)
155.	Wysyłanie wyników skanowania offline na serwer FTP (Audyt)	spełnia / nie spełnia *)
156.	Przekazywanie konfiguracji wzorcowej dla skanera offline	spełnia / nie spełnia *)
157.	Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania	spełnia / nie spełnia *)
158.	Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy	spełnia / nie spełnia *)
159.	Określanie masek plików dla publikacji elektronicznych (e-book)	spełnia / nie spełnia *)
160.	Skan plików skompresowanych	spełnia / nie spełnia *)
161.	Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz	spełnia / nie spełnia *)
162.	Odczyt skrótów MD5, SHA-1, SHA256, SHA384, SHA512 plików	spełnia / nie spełnia *)
163.	Wbudowane profile skanowania (np. profil wzorcowy)	spełnia / nie spełnia *)
164.	Definicja własnych ustawień skanowania	spełnia / nie spełnia *)
165.	Porównywanie wyników skanowania oprogramowania	spełnia / nie spełnia *)
166.	Wykrywanie plików multimedialnych	spełnia / nie spełnia *)
167.	Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)	spełnia / nie spełnia *)
168.	Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI	spełnia / nie spełnia *)
169.	Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie	spełnia / nie spełnia *)
170.	Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji/pakietów/systemów operacyjnych	spełnia / nie spełnia *)
171.	Nadpisanie bazy wzorców najnowszą oficjalną bazą producenta	spełnia / nie spełnia *)
172.	Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)	spełnia / nie spełnia *)
Audyt oprogramowania		
173.	Rozliczanie pakietów aplikacji	spełnia / nie spełnia *)
174.	Rozliczanie systemów operacyjnych	spełnia / nie spełnia *)
175.	Rozliczanie licencji typu „downgrade”, „upgrade” oraz instalacji innego oprogramowania w ramach licencji	spełnia / nie spełnia *)
176.	Audyt oprogramowania rozliczany automatycznie – informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
177.	Historia audytów (wyniki audytów są przechowywane w bazie danych – można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)	spełnia / nie spełnia *)
178.	Wsparcie procesu audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę	spełnia / nie spełnia *)
179.	Gotowe metryki audytowanego komputera – załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)	spełnia / nie spełnia *)
180.	Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji	spełnia / nie spełnia *)
181.	Statystyki wykonanych audytów	spełnia / nie spełnia *)
Funkcje		
182.	Mechanizm informujący o nowej bazie wzorców oprogramowania	spełnia / nie spełnia *)
183.	Definiowanie własnych wzorców oprogramowania	spełnia / nie spełnia *)
184.	Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych	spełnia / nie spełnia *)
185.	Automatyczna klasyfikacja używanych programów z wykorzystaniem AI	spełnia / nie spełnia *)
186.	Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania	spełnia / nie spełnia *)
187.	Wykrywanie kluczy/identyfikatorów programów	spełnia / nie spełnia *)
188.	W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza	spełnia / nie spełnia *)
189.	Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office	spełnia / nie spełnia *)
190.	Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania	spełnia / nie spełnia *)
191.	Zbiorcze raporty wyników skanowania oprogramowania – Pakiety, pliki, systemy operacyjne, klucze zainstalowanych aplikacji	spełnia / nie spełnia *)
192.	Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.	spełnia / nie spełnia *)
193.	Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.	spełnia / nie spełnia *)
194.	„Wielkie raporty” (możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)	spełnia / nie spełnia *)
195.	Zdalna instalacja oraz aktualizacja z katalogu oprogramowania Winget	spełnia / nie spełnia *)
196.	Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)	spełnia / nie spełnia *)
197.	Zdalna dezinstalacja oprogramowania	spełnia / nie spełnia *)
198.	Utworzenie harmonogramu dezinstalacji oprogramowania	spełnia / nie spełnia *)
199.	Generowanie skryptu dezinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania	spełnia / nie spełnia *)
200.	Raport stanu oprogramowania antywirusowego, antyszpiegowskiego oraz zapory sieciowej	spełnia / nie spełnia *)
201.	Raport zainstalowanych aktualizacji systemu Windows	spełnia / nie spełnia *)
C. Kontrola wykorzystania sprzętu i oprogramowania (monitoring użytkowników)		
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne		
202.	Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) – jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach	spełnia / nie spełnia *)
203.	Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup, do których konto należy	spełnia / nie spełnia *)
204.	Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
205.	Określanie firmy, do której należy użytkownik	spełnia / nie spełnia *)
206.	Określanie przełożonego dla użytkownika	spełnia / nie spełnia *)
207.	Prezentacja „stanu użytkownika” (obecny, nieobecny, nowy)	spełnia / nie spełnia *)
208.	Prezentacja 'statusu użytkownika' (zatrudniony, zwolniony itd.)	spełnia / nie spełnia *)
209.	Zarządzanie stanowiskami użytkowników	spełnia / nie spełnia *)
210.	Przeniesienie rekordu użytkownika do archiwum	spełnia / nie spełnia *)
211.	Automatyczne generowanie historii zmian rekordu użytkownika (historia użytkownika)	spełnia / nie spełnia *)
212.	Odczytywanie informacji o użytkownikach z Active Directory oraz Entra ID	spełnia / nie spełnia *)
213.	Pełna synchronizacja rekordów użytkowników (odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz Entra ID)	spełnia / nie spełnia *)
214.	Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień	spełnia / nie spełnia *)
215.	Podgląd zdjęcia przypisanego do użytkownika	spełnia / nie spełnia *)
216.	Przypisywanie do użytkownika załączników (pliki)	spełnia / nie spełnia *)
217.	Przypisywanie notatek do użytkownika	spełnia / nie spełnia *)
218.	Ewidencja zdarzeń przypisanych do użytkowników	spełnia / nie spełnia *)
219.	Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory	spełnia / nie spełnia *)
Raporty		
220.	Analiza aktywności użytkowników	spełnia / nie spełnia *)
221.	Grupowanie danych według komputerów, jeśli użytkownik wykorzystywał więcej niż jedno stanowisko	spełnia / nie spełnia *)
222.	Analiza zdarzeń sesji użytkownika (logowanie, wylogowanie, zablokowanie, odblokowanie, nawiązanie połączenia RDP, zakończenie połączenia RDP)	spełnia / nie spełnia *)
223.	Analiza przerw w pracy	spełnia / nie spełnia *)
224.	Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)	spełnia / nie spełnia *)
225.	Analiza aktywności mikrofonu oraz kamery	spełnia / nie spełnia *)
226.	Analiza wykorzystania poszczególnych aplikacji w czasie	spełnia / nie spełnia *)
227.	Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie	spełnia / nie spełnia *)
228.	Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika	spełnia / nie spełnia *)
229.	Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny)	spełnia / nie spełnia *)
230.	Statystyki najczęściej wykorzystywanych aplikacji	spełnia / nie spełnia *)
231.	Statystyki wykorzystania komputerów przez poszczególnych użytkowników	spełnia / nie spełnia *)
232.	Statystyki aktywności użytkownika i grup użytkowników	spełnia / nie spełnia *)
233.	Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin	spełnia / nie spełnia *)
234.	Kontrola wydruków – historia zadań drukowania zainicjowanych przez poszczególnych użytkowników	spełnia / nie spełnia *)
235.	Kontrola wydruków – monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)	spełnia / nie spełnia *)
236.	Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz.-b./kolor, dpi)	spełnia / nie spełnia *)
237.	Monitoring wydruków na drukarkach sieciowych	spełnia / nie spełnia *)
238.	Monitoring użytkowników stacji terminalowych	spełnia / nie spełnia *)
239.	Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
240.	Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca	spełnia / nie spełnia *)
241.	Raport zbiorczy historii zmian w rekordach użytkowników	spełnia / nie spełnia *)
242.	Raport podsumowania aktywności użytkowników	spełnia / nie spełnia *)
243.	Eksport danych czasu pracy z podziałem na czas pozytywny, neutralny i negatywny	spełnia / nie spełnia *)
244.	Uwzględnienie dni tygodnia w raportach monitoringu użytkowników	spełnia / nie spełnia *)
245.	Analiza odwiedzanych stron oraz kategorii odwiedzonych stron	spełnia / nie spełnia *)
Funkcje		
246.	Blokada niepożądanych aplikacji – programy mogą być blokowane dla całej organizacji lub tylko dla wybranych użytkowników	spełnia / nie spełnia *)
247.	Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń	spełnia / nie spełnia *)
248.	Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych	spełnia / nie spełnia *)
249.	Automatycznie budowana baza informacji o napędach zewnętrznych	spełnia / nie spełnia *)
250.	Automatyczna rejestracja wykrytych dysków zewnętrznych	spełnia / nie spełnia *)
251.	Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)	spełnia / nie spełnia *)
252.	Odczyt i blokada urządzeń PTP/MTP	spełnia / nie spełnia *)
253.	Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM	spełnia / nie spełnia *)
254.	Komunikacja z użytkownikami (komunikator, e-mail) bezpośrednio z zakładki Użytkownicy	spełnia / nie spełnia *)
255.	Informacje o ostatnio zalogowanych osobach na stacjach klienckich	spełnia / nie spełnia *)
256.	Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje	spełnia / nie spełnia *)
257.	Komentowanie przerw pracy	spełnia / nie spełnia *)
258.	Akceptacja / odrzucenie przerwy w pracy na podstawie komentarza użytkownika	spełnia / nie spełnia *)
259.	Akceptacja przerw pracy przez przełożonych	spełnia / nie spełnia *)
260.	Automatyczne wykrywanie przerw w pracy (na podstawie aktywności użytkownika)	spełnia / nie spełnia *)
D. Kontrola wykorzystania Internetu		
Funkcje		
261.	Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)	spełnia / nie spełnia *)
262.	Blokada pobierania plików wg typu MIME	spełnia / nie spełnia *)
263.	Blokada stron internetowych dla protokołu HTTP/HTTPS w najpopularniejszych przeglądarkach WWW	spełnia / nie spełnia *)
264.	Kategoryzacja stron internetowych	spełnia / nie spełnia *)
265.	Import stron WWW z pliku lub ze schowka	spełnia / nie spełnia *)
266.	Słowniki kategorii stron WWW	spełnia / nie spełnia *)
267.	Blokada dostępu do witryn zgodnie z harmonogramem	spełnia / nie spełnia *)
268.	Blokada dostępu do witryn na podstawie kategorii strony WWW	spełnia / nie spełnia *)
269.	Blokada trybu incognito w przeglądarce Google Chrome	spełnia / nie spełnia *)
Raporty		
270.	Raporty dotyczące aktywności użytkowników w Internecie	spełnia / nie spełnia *)
271.	Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
272.	Monitoring stron internetowych dla protokołu HTTP/HTTPS (Przeglądarki oparte o silnik Chromium, Edge, Chrome, Vivaldi, Firefox)	spełnia / nie spełnia *)
273.	Analiza liczby wejść na poszczególne strony lub domeny	spełnia / nie spełnia *)
274.	Kategoryzacja odwiedzanych domen i stron, opcjonalnie z wykorzystaniem AI	spełnia / nie spełnia *)
275.	Raport informujący o plikach pobranych przez przeglądarki WWW	spełnia / nie spełnia *)
276.	Raport informujący o danych wysłanych przez przeglądarki (bez Firefox)	spełnia / nie spełnia *)
277.	Monitoring plików pobieranych przez przeglądarki internetowe	spełnia / nie spełnia *)
E. Helpdesk		
Obsługa zgłoszeń		
278.	Rejestracja i obsługa zgłoszeń	spełnia / nie spełnia *)
279.	Obsługa zgłoszeń w modelu Kanban	spełnia / nie spełnia *)
280.	Określanie relacji pomiędzy zgłoszeniami (np. kopia, incydent nadrzędny)	spełnia / nie spełnia *)
281.	Edycja zgłoszeń powiązanych w oknie bieżącego zgłoszenia	spełnia / nie spełnia *)
282.	Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii	spełnia / nie spełnia *)
283.	Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów	spełnia / nie spełnia *)
284.	Opis zgłoszenia w formacie HTML	spełnia / nie spełnia *)
285.	Nawiązywanie połączeń zdalnych bezpośrednio z edytora zgłoszenia	spełnia / nie spełnia *)
286.	Tworzenie notatek dla zgłoszeń	spełnia / nie spełnia *)
287.	Zapisywanie wersji roboczej komentarza	spełnia / nie spełnia *)
288.	Archiwizacja zgłoszeń	spełnia / nie spełnia *)
289.	Monitoring czasu pracy nad incydentem (ang. time tracking)	spełnia / nie spełnia *)
290.	Raport ewidencji czasu pracy nad zgłoszeniem	spełnia / nie spełnia *)
291.	Informacja o czasie reakcji do podjęcia zgłoszenia	spełnia / nie spełnia *)
292.	Dodanie prywatnego komentarza	spełnia / nie spełnia *)
293.	Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia	spełnia / nie spełnia *)
294.	Dodanie załączników do incydentów, również do komentarza	spełnia / nie spełnia *)
295.	Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie	spełnia / nie spełnia *)
296.	Określanie uprawnień do incydentów (publiczne, prywatne, dla określonych działów)	spełnia / nie spełnia *)
297.	Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń	spełnia / nie spełnia *)
298.	Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń	spełnia / nie spełnia *)
299.	Wydruk historii zgłoszenia	spełnia / nie spełnia *)
300.	Widok kalendarza (planowanie rozwiązania incydentów)	spełnia / nie spełnia *)
301.	Korelacja incydentu z elementem zasobów	spełnia / nie spełnia *)
302.	Raport zbiorczy historii zmian	spełnia / nie spełnia *)
303.	Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej	spełnia / nie spełnia *)
304.	Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania	spełnia / nie spełnia *)
305.	Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA	spełnia / nie spełnia *)
306.	Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu	spełnia / nie spełnia *)
307.	Określenie wpływu biznesowego wybranego zgłoszenia	spełnia / nie spełnia *)
308.	Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń e-mail	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
309.	Duplikacja i replikacja zgłoszeń	spełnia / nie spełnia *)
310.	Powiadomienia o liczbie nieprzeczytanych zgłoszeń	spełnia / nie spełnia *)
311.	Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł	spełnia / nie spełnia *)
312.	Asystent AI do generowania odpowiedzi, podsumowania zgłoszenia, tłumaczeń, generowania tagów oraz wykrywania kategorii zgłoszeń	spełnia / nie spełnia *)
313.	Obsługa formatu Markdown w asystencie AI	spełnia / nie spełnia *)
314.	Podsumowania zgłoszeń generowane przez AI	spełnia / nie spełnia *)
315.	Podsumowania komentarzy generowane przez AI	spełnia / nie spełnia *)
Konfiguracja helpdesk		
316.	Architektura drzewa dla kategorii zgłoszeń	spełnia / nie spełnia *)
317.	Tworzenie szablonów odpowiedzi	spełnia / nie spełnia *)
318.	Cykliczne raportowanie listy incydentów	spełnia / nie spełnia *)
319.	Tworzenie własnych dodatkowych atrybutów dla zgłoszeń	spełnia / nie spełnia *)
320.	Tworzenie i zarządzanie typami statusów zgłoszeń	spełnia / nie spełnia *)
321.	Personalizowane szablony wiadomości e-mail z możliwością ustawienia stałego załącznika	spełnia / nie spełnia *)
322.	Notyfikacje e-mail o utworzeniu/zmianie/usunięciu incydentu	spełnia / nie spełnia *)
323.	Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)	spełnia / nie spełnia *)
324.	Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)	spełnia / nie spełnia *)
325.	Weryfikacja rozmiaru załącznika wiadomości e-mail	spełnia / nie spełnia *)
326.	Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)	spełnia / nie spełnia *)
327.	Możliwość filtrowania adresów e-mail w importerze wiadomości e-mail	spełnia / nie spełnia *)
328.	Obsługa wielu kont pocztowych (import + notyfikacje e-mail)	spełnia / nie spełnia *)
329.	Tworzenie własnych trybów oraz priorytetów incydentów	spełnia / nie spełnia *)
330.	Personalizacja widoku raportu listy incydentów	spełnia / nie spełnia *)
331.	Profile zgłaszających w helpdesk	spełnia / nie spełnia *)
332.	Personalizacja kolorów statusów zgłoszeń	spełnia / nie spełnia *)
333.	Automatyczne przypisywanie zgłoszeń do użytkowników	spełnia / nie spełnia *)
334.	Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego	spełnia / nie spełnia *)
335.	Konfiguracja maksymalnej wielkości załącznika	spełnia / nie spełnia *)
336.	Możliwość rejestrowania informacji o wyświetleniu zgłoszenia w historii	spełnia / nie spełnia *)
Moduł połączeń zdalnych		
337.	Operacje na plikach i katalogach	spełnia / nie spełnia *)
338.	Zarządzanie procesami i rejestrem	spełnia / nie spełnia *)
339.	Monitoring pracy wykonywanej na komputerze	spełnia / nie spełnia *)
340.	Zdalny podgląd pulpitów wielu stacji	spełnia / nie spełnia *)
341.	Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji	spełnia / nie spełnia *)
342.	Wysyłanie wiadomości do użytkowników	spełnia / nie spełnia *)
343.	Uruchamianie na stacjach programów z wiersza poleceń	spełnia / nie spełnia *)
344.	Zdalne uruchamianie komputera za pomocą funkcji Wake-on-LAN	spełnia / nie spełnia *)
345.	Wake-on-LAN pozwala na definicję portu oraz adresu komputera docelowego	spełnia / nie spełnia *)
346.	Przejęcie kontroli nad stacją roboczą	spełnia / nie spełnia *)
347.	Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego	spełnia / nie spełnia *)
348.	Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
349.	Przejęcie kontroli nad komputerem bez zalogowanego użytkownika	spełnia / nie spełnia *)
350.	Wysyłanie pytania o zgodę na zdalny dostęp lub wysłanie komunikatu z informacją o rozpoczęciu podglądu pulpitu	spełnia / nie spełnia *)
351.	Podgląd pulpitu zdalnego w osobnym oknie z opcją full-screen	spełnia / nie spełnia *)
352.	Obsługa wielu monitorów dla podglądu pulpitu	spełnia / nie spełnia *)
353.	Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu	spełnia / nie spełnia *)
354.	Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie	spełnia / nie spełnia *)
355.	Połączenie pulpitem zdalnym w konfiguracji NAT-NAT	spełnia / nie spełnia *)
356.	Zarządzanie usługami systemu Windows	spełnia / nie spełnia *)
357.	Raport sesji zdalnego pulpitu	spełnia / nie spełnia *)
358.	Wybór adresu IP, na którym ma być zestawione połączenie zdalne	spełnia / nie spełnia *)
359.	Wybór portu, na którym klient nasłuchuje połączenia zdalnego	spełnia / nie spełnia *)
360.	Wykorzystanie własnego protokołu producenta lub MS RDP do połączeń zdalnych	spełnia / nie spełnia *)
361.	Obsługa wiersza poleceń / PowerShell w trybie live	spełnia / nie spełnia *)
362.	Raport sesji wiersza poleceń	spełnia / nie spełnia *)
363.	Blokada kopiowania danych ze schowka operatora na komputer zdalny	spełnia / nie spełnia *)
364.	Blokada połączeń w trybie informowania / cichym	spełnia / nie spełnia *)
Baza wiedzy		
365.	Wbudowana baza wiedzy	spełnia / nie spełnia *)
366.	Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk	spełnia / nie spełnia *)
367.	Kopiowanie artykułów	spełnia / nie spełnia *)
368.	Edytor HTML	spełnia / nie spełnia *)
369.	Osadzanie załączników w treści artykułów	spełnia / nie spełnia *)
370.	Osadzanie multimediów w treści artykułów	spełnia / nie spełnia *)
371.	Baza wiedzy pozwala na tworzenie artykułów prywatnych oraz publicznych	spełnia / nie spełnia *)
372.	Szybkie kopiowanie wpisów bazy wiedzy	spełnia / nie spełnia *)
373.	Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk	spełnia / nie spełnia *)
374.	Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów	spełnia / nie spełnia *)
375.	Informacja o liczbie odsłon artykułu bazy wiedzy	spełnia / nie spełnia *)
376.	Bezpośrednie linkowanie artykułów bazy wiedzy	spełnia / nie spełnia *)
SLA		
377.	Definiowanie planów umów SLA	spełnia / nie spełnia *)
378.	Definiowanie czasu obowiązywania umów SLA	spełnia / nie spełnia *)
379.	Definiowanie czasu pracy działów wsparcia technicznego	spełnia / nie spełnia *)
380.	Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych	spełnia / nie spełnia *)
381.	Definiowanie czasów reakcji oraz realizacji zgłoszenia	spełnia / nie spełnia *)
382.	Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji	spełnia / nie spełnia *)
383.	Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie	spełnia / nie spełnia *)
384.	Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA	spełnia / nie spełnia *)
F. Centralne repozytorium załączników		
Funkcje		
385.	Załączniki przechowywane w centralnym repozytorium	spełnia / nie spełnia *)
386.	Utworzenie relacji załącznika z innymi elementami systemu 1–N (jeden do wielu)	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
387.	Dodawanie i modyfikacja załączników z poziomu innych zasobów	spełnia / nie spełnia *)
388.	Załączniki typu: link, udział oraz plik	spełnia / nie spełnia *)
389.	Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura	spełnia / nie spełnia *)
390.	Historia zmian załącznika	spełnia / nie spełnia *)
G. Zarządzanie użytkownikami		
Funkcje		
391.	Raportowanie aktywności pracy	spełnia / nie spełnia *)
392.	Przeglądanie ostatnio zgłoszonych incydentów	spełnia / nie spełnia *)
393.	Powiązanie użytkownika z licencją	spełnia / nie spełnia *)
394.	Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów	spełnia / nie spełnia *)
395.	Cykliczne, automatyczne generowanie i dystrybucja mailowa raportów	spełnia / nie spełnia *)
396.	Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze	spełnia / nie spełnia *)
397.	Zgłoszenia dotyczące wniosków nieobecności użytkowników	spełnia / nie spełnia *)
398.	Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności	spełnia / nie spełnia *)
399.	Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika	spełnia / nie spełnia *)
400.	Automatyczne utworzenie relacji przełożony – podwładny na podstawie skanów Active Directory	spełnia / nie spełnia *)
401.	Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO	spełnia / nie spełnia *)
402.	Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych	spełnia / nie spełnia *)
403.	Planowanie dni wolnych w widoku kalendarza	spełnia / nie spełnia *)
404.	Planowanie zastępstw podczas nieobecności	spełnia / nie spełnia *)
405.	Blokowanie kont Windows	spełnia / nie spełnia *)
H. Raportowanie cykliczne		
Raporty automatyczne, wysyłane e-mailem zgodnie z określonym harmonogramem oraz listą odbiorców:		
Użytkownicy		
406.	Raport historii sesji	spełnia / nie spełnia *)
407.	Raport nośników danych	spełnia / nie spełnia *)
408.	Raport operacji na plikach	spełnia / nie spełnia *)
409.	Raport wydruków	spełnia / nie spełnia *)
410.	Raport użycia aplikacji	spełnia / nie spełnia *)
411.	Raport nagłówków okien [z możliwością wyłączenia]	spełnia / nie spełnia *)
412.	Raport odwiedzonych stron WWW	spełnia / nie spełnia *)
413.	Raport najczęściej odwiedzanych stron internetowych	spełnia / nie spełnia *)
414.	Raport wysyłanych plików	spełnia / nie spełnia *)
415.	Raport czasu pracy przy komputerze	spełnia / nie spełnia *)
416.	Raport agregujący statystyki użytkownika w rozbiciu godzinowym / kalendarzowym	spełnia / nie spełnia *)
Zasoby		
417.	Raport historii zasobów	spełnia / nie spełnia *)
418.	Raport informujący o nowych zasobach	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
419.	Raport informujący o nadchodzących terminach w zasobach	spełnia / nie spełnia *)
420.	Raport zasobów zarchiwizowanych	spełnia / nie spełnia *)
421.	Raport systemów operacyjnych	spełnia / nie spełnia *)
Podstawowe		
422.	Raport informacji o autoryzowanych agentach	spełnia / nie spełnia *)
Oprogramowanie		
423.	Raport zainstalowanego oprogramowania	spełnia / nie spełnia *)
424.	Raport szczegółów plików	spełnia / nie spełnia *)
Helpdesk		
425.	Raport incydentów (Helpdesk)	spełnia / nie spełnia *)
426.	Raport czasu pracy nad zgłoszeniem	spełnia / nie spełnia *)
427.	Raport czasów SLA, obejmujący: czasy SLA, czas realizacji, historię zgłoszeń	spełnia / nie spełnia *)
I. Automatyzacja		
Akcje (modyfikacje obiektów systemu, skrypty, powiadomienia mail / SMS / pop-up) wykonywane w przypadku wystąpienia wybranych wyzwalaczy.		
Wyzwalacze reguł – ogólne		
428.	Zakończenie okresu wsparcia producenta (asysty serwisowej)	spełnia / nie spełnia *)
429.	Wygaśnięcie certyfikatu SSL	spełnia / nie spełnia *)
430.	Kończące się licencje na agenta	spełnia / nie spełnia *)
431.	Zapełniona baza danych	spełnia / nie spełnia *)
432.	Dziennik operacji (uruchamiana po dodaniu wpisów do dziennika operacji)	spełnia / nie spełnia *)
433.	Zbyt duży rozmiar folderu cache	spełnia / nie spełnia *)
434.	Wygaśnięcie tokenu autoryzacyjnego API	spełnia / nie spełnia *)
Wyzwalacze reguł – zasoby		
435.	Brak połączenia agenta	spełnia / nie spełnia *)
436.	Brak wolnej przestrzeni na dysku	spełnia / nie spełnia *)
437.	Ostrzeżenie od Windows Security Center	spełnia / nie spełnia *)
438.	Zakończenie skanowania sprzętu	spełnia / nie spełnia *)
439.	Powielenie agenta	spełnia / nie spełnia *)
440.	Podłączenie dysku zewnętrznego	spełnia / nie spełnia *)
441.	Stan modułu TPM	spełnia / nie spełnia *)
442.	Stan szyfrowania woluminów	spełnia / nie spełnia *)
443.	Dodanie zasobu	spełnia / nie spełnia *)
444.	Zmiana zasobu	spełnia / nie spełnia *)
445.	Usunięcie zasobu	spełnia / nie spełnia *)
446.	Zakończenie okresu gwarancyjnego	spełnia / nie spełnia *)
447.	Zakończenie umowy serwisowej	spełnia / nie spełnia *)
448.	Powielenie zasobów	spełnia / nie spełnia *)
449.	Nowy wpis w dzienniku zdarzeń Windows	spełnia / nie spełnia *)
Wyzwalacze reguł – oprogramowanie		
450.	Zmiana oprogramowania	spełnia / nie spełnia *)
451.	Zakończenie skanowania oprogramowania	spełnia / nie spełnia *)
452.	Zakończenie okresu wsparcia technicznego	spełnia / nie spełnia *)
453.	Zamknięcie audytu	spełnia / nie spełnia *)
Wyzwalacze reguł – licencje		

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
454.	Dodanie licencji	spełnia / nie spełnia *)
455.	Zmiana licencji	spełnia / nie spełnia *)
456.	Usunięcie licencji	spełnia / nie spełnia *)
457.	Wygaśnięcie licencji	spełnia / nie spełnia *)
458.	Planowana wymiana licencji	spełnia / nie spełnia *)
Wyzwalacze reguł – użytkownicy		
459.	Dodanie użytkownika	spełnia / nie spełnia *)
460.	Zmiana użytkownika	spełnia / nie spełnia *)
461.	Usunięcie użytkownika	spełnia / nie spełnia *)
462.	Logowanie użytkownika	spełnia / nie spełnia *)
463.	Wylogowanie użytkownika	spełnia / nie spełnia *)
464.	Strony WWW	spełnia / nie spełnia *)
465.	Nagłówki okien	spełnia / nie spełnia *)
Wyzwalacze reguł – helpdesk		
466.	Dodanie zgłoszenia	spełnia / nie spełnia *)
467.	Usunięcie zgłoszenia	spełnia / nie spełnia *)
468.	Zmiana zgłoszenia	spełnia / nie spełnia *)
469.	Zapisana wersja robocza	spełnia / nie spełnia *)
470.	Brak aktywności w zgłoszeniu	spełnia / nie spełnia *)
Wyzwalacze reguł – RODO		
471.	Zbliżający się koniec dostępu	spełnia / nie spełnia *)
Akcje reguł		
472.	Wykonywanie skryptu na podstawie zdefiniowanej reguły	spełnia / nie spełnia *)
473.	Wysłanie powiadomienia w konsoli administracyjnej / portalu WWW na podstawie zdefiniowanej reguły	spełnia / nie spełnia *)
474.	Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)	spełnia / nie spełnia *)
475.	Modyfikacja zasobu / użytkownika / zgłoszenia – w zależności od reguły	spełnia / nie spełnia *)
476.	Dodanie komentarza (dla reguł Helpdesk) [możliwe osobne reakcje na komentarz zgłaszającego / rozwiązującego]	spełnia / nie spełnia *)
477.	Wysyłka wiadomości SMS	spełnia / nie spełnia *)
478.	Wysyłka powiadomień do Microsoft Teams	spełnia / nie spełnia *)
479.	Przypisanie atrybutu	spełnia / nie spełnia *)
480.	Przypisanie / usunięcie reguł dostępu WWW	spełnia / nie spełnia *)
481.	Podsumowanie zgłoszenia z wykorzystaniem AI	spełnia / nie spełnia *)
Akcje reguł – funkcje ogólne		
482.	Uruchamianie reguł w harmonogramie	spełnia / nie spełnia *)
O. API		
624.	API – moduł Firmy: pobieranie informacji o strukturze firm	spełnia / nie spełnia *)
625.	API – moduł Lokalizacje: pobieranie listy lokalizacji	spełnia / nie spełnia *)
626.	API – moduł Struktura organizacyjna: pobieranie widoku grup struktury organizacyjnej	spełnia / nie spełnia *)
627.	API – moduł Użytkownicy: pobieranie danych użytkowników; aktualizacja użytkowników; pobieranie historii zmian użytkowników	spełnia / nie spełnia *)

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	Spełnienie wymagań minimalnych
628.	API – moduł Zasoby: pobieranie informacji o zasobach; tworzenie zasobów; aktualizacja zasobów; pobieranie historii zmian zasobów; pobieranie statusów zasobów; pobieranie typów zasobów; pobieranie typów kodów kreskowych	spełnia / nie spełnia *)
629.	API – moduł Załączniki: pobieranie załączników; tworzenie załączników plikowych; tworzenie załączników typu link	spełnia / nie spełnia *)
630.	API – moduł Helpdesk: pobieranie zgłoszeń; tworzenie zgłoszeń; aktualizacja zgłoszeń; tworzenie komentarzy do zgłoszeń; pobieranie historii zmian zgłoszeń; pobieranie ewidencji czasu pracy nad zgłoszeniem; pobieranie kategorii, atrybutów, trybów, ważności, priorytetów i statusów zgłoszeń; pobieranie statusów dostępnych przy tworzeniu zgłoszenia; pobieranie ustawień rozwiązujących; pobieranie definicji umów SLA; pobieranie ustawień kont pocztowych	spełnia / nie spełnia *)
P. Architektura i wymagania techniczne		
631.	Kreator instalacyjny ułatwiający wdrożenie systemu	spełnia / nie spełnia *)
632.	Aplikacje konsoli administracyjnej (Master), serwera (Server) i agenta (Agent) w wersji x64	spełnia / nie spełnia *)
633.	Aplikacja dla urządzeń mobilnych	spełnia / nie spełnia *)
634.	Interfejs użytkownika dostępny w wielu językach, w tym w języku polskim	spełnia / nie spełnia *)
635.	Rozproszona architektura systemu: serwer, konsola administracyjna, agent – z możliwością pracy każdego z komponentów na różnych komputerach	spełnia / nie spełnia *)
636.	Praca w oparciu o MS SQL Server oraz MS SQL Express (2012 lub nowszy)	spełnia / nie spełnia *)
637.	Praca w oparciu o PostgreSQL 11 lub nowszy	spełnia / nie spełnia *)
638.	Szyfrowane połączenie pomiędzy serwerem aplikacji a bazą danych	spełnia / nie spełnia *)
639.	Możliwość uruchomienia wielu równoległych instancji systemu	spełnia / nie spełnia *)
640.	Obsługa systemów operacyjnych przez agenta: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11	spełnia / nie spełnia *)
641.	Obsługa systemów operacyjnych przez konsolę administracyjną: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11	spełnia / nie spełnia *)
642.	Obsługa systemów operacyjnych przez serwer: Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, Windows 7, 8, 10, 11 oraz Linux	spełnia / nie spełnia *)
643.	Wszystkie wykonywalne komponenty systemu podpisane certyfikatem Code Signing (Microsoft Authenticode) wydanym przez zaufany urząd certyfikacji	spełnia / nie spełnia *)
644.	Sterowniki systemowe podpisane certyfikatem EV Code Signing (Extended Validation), umożliwiające pracę w 64-bitowych systemach operacyjnych Microsoft Windows	spełnia / nie spełnia *)

*) niepotrzebne skreślić. Niespełnienie któregokolwiek z wymagań minimalnych skutkuje odrzuceniem oferty jako niezgodnej z warunkami zamówienia.

4. Wsparcie producenta

4.1. Wykonawca zapewni wsparcie producenta (asystę serwisową) dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji.

4.2. W ramach wsparcia Zamawiający otrzyma co najmniej: aktualizacje posiadanej wersji oprogramowania, prawo do aktualizacji do kolejnych wersji (upgrade), aktualizacje bazy wzorców oprogramowania, dostęp do bazy wiedzy i dokumentacji producenta oraz pomoc techniczną. Dla instancji OT producent musi udostępniać aktualizacje oprogramowania i bazy wzorców w postaci pakietów do instalacji w trybie offline.

4.3. Zgłoszenia przyjmowane są w dni robocze, przez portal producenta, e-mailem lub telefonicznie, w języku polskim. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych.

5. Wdrożenie w sieciach IT i OT

5.1. Zasady wdrożenia w sieciach IT i OT

5.1.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję Systemu, zgodnie z pkt 2.8.

5.12. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

5.1.3. W sieci OT agent zostanie zainstalowany wyłącznie na komputerach z systemem Windows wskazanych przez Zamawiającego na piśmie (np. stacje operatorskie HMI, stacje inżynierskie, serwery systemów nadrzędnych), po potwierdzeniu przez Zamawiającego, że instalacja nie narusza warunków wsparcia ani certyfikacji systemu sterowania. Agent nie będzie instalowany na urządzeniach sterowania procesem (m.in. sterownikach PLC i RTU).

5.1.4. W instancji OT Wykonawca skonfiguruje System w sposób bezpieczny dla procesu technologicznego, w szczególności:

- aktywne skanowanie sieci (pkt 2 tabeli) zostanie ograniczone do zakresów adresowych wskazanych przez Zamawiającego, z wyłączeniem segmentów z urządzeniami sterowania procesem, i będzie uruchamiane wyłącznie w uzgodnionych oknach serwisowych;
- funkcje mogące wpływać na pracę stacji – zarządzanie zasilaniem (pkt 83–91 tabeli), zdalne wykonywanie skryptów, zdalna instalacja i dezinstalacja oprogramowania, blokada aplikacji oraz przejęcie kontroli nad stacją – zostaną wyłączone albo udostępnione wyłącznie wskazanym administratorom, z obowiązkiem ręcznego uruchomienia;
- funkcje monitorowania aktywności użytkowników (sekcje C i D, pkt 202–260 i 261–277 tabeli) zostaną skonfigurowane w zakresie wskazanym przez Zamawiającego;
- zostanie włączona kontrola nośników zewnętrznych i urządzeń PTP/MTP (pkt 247–253 tabeli), z listą nośników autoryzowanych uzgodnioną z Zamawiającym;
- funkcje wymagające dostępu do Internetu lub usług chmurowych (pkt 2.4) zostaną wyłączone.

5.1.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym. Instalacja agenta w sieci OT zostanie poprzedzona instalacją pilotażową na stacji wskazanej przez Zamawiającego.

5.2. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

5.2.1. Przeprowadzenie analizy przedwdrożeniowej oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, zawierającego architekturę, wymagania dla serwerów i bazy danych, zakres modułów i funkcji, polityki agentów, uprawnienia oraz harmonogram prac, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

5.2.2. Instalacja i konfiguracja serwera aplikacji, bazy danych, konsoli administracyjnej i portalu WWW w każdej z instancji, w tym szyfrowanie komunikacji (TLS), konfiguracja kont i ról, uwierzytelniania wieloskładnikowego i polityki haseł, kopii zapasowych bazy danych oraz utwardzenie konfiguracji (zmiana domyślnych haseł, wyłączenie zbędnych usług).

5.2.3. Integracja instancji IT z usługami katalogowymi Zamawiającego (Active Directory, Microsoft Entra ID / Intune), serwerem poczty i skrzynkami helpdesk **jeśli dotyczy**. Instancja OT zostanie zintegrowana wyłącznie z usługami działającymi w sieci OT.

5.2.4. Dystrybucja agentów na stanowiska wskazane przez Zamawiającego (w sieci IT – co najmniej **20** stanowisk, w sieci OT – stanowiska wskazane zgodnie z pkt 5.2.3), wykonanie inwentaryzacji sprzętu i oprogramowania oraz weryfikacja poprawności danych.

5.2.5. Konfiguracja modułów zgodnie z projektem, w tym: struktury organizacyjnej i lokalizacji, typów i statusów zasobów, licencji oraz pierwszego audytu legalności oprogramowania, reguł automatyzacji i powiadomień.

5.2.6. Przeprowadzenie testów odbiorczych w każdej z sieci, według scenariuszy przedłożonych Zamawiającemu do akceptacji, obejmujących co najmniej:

- inwentaryzację sprzętu i oprogramowania na stanowiskach testowych oraz wykonanie audytu legalności oprogramowania;
- wyzwolenie reguły automatyzacji (np. brak połączenia agenta) i dostarczenie powiadomienia;
- aktualizację instancji OT w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu zarządzania oraz brak połączeń między instancjami IT i OT.

5.2.7. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej: opis architektury i konfiguracji, wykaz serwerów, kont technicznych i ról, opis polityk agentów i reguł automatyzacji, protokoły z testów oraz procedury administracyjne (instalacja agenta, aktualizacja – dla sieci OT również w trybie offline, kopia zapasowa i odtworzenie bazy danych). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

5.2.8. Przeprowadzenie w siedzibie Zamawiającego instruktażu dla administratorów w wymiarze nie mniejszym niż **8** godzin dla maksymalnie **2** osób, obejmującego obsługę obu instancji oraz procedury z pkt 5.3.7.

5.2.9. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT oraz danych osobowych przetwarzanych w Systemie. W zakresie, w jakim Wykonawca uzyska dostęp do danych osobowych, strony zawrą umowę powierzenia przetwarzania danych osobowych.

5.2.10. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

6. Terminy realizacji i odbiór

6.1. Termin realizacji zamówienia: do **14** dni od podpisania umowy.

6.2. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji oraz potwierdzenia rejestracji wsparcia producenta.

6.3. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 5.2.6 oraz przekazaniu dokumentacji z pkt 5.2.7. Po odbiorze wdrożenia w obu sieciach i przeprowadzeniu instruktażu strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazanie w OPZ nazw systemów, usług i technologii, z którymi oferowane oprogramowanie musi współpracować (m.in. Microsoft Windows, Active Directory, Microsoft Entra ID, Intune, Microsoft Teams, MS SQL Server, PostgreSQL, Winget, Dell), wynika z infrastruktury wykorzystywanej przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

7.2. Pozostałe nazwy własne, znaki towarowe lub normy wskazane w OPZ mają charakter przykładowy. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo

zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.

7.3 Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne".

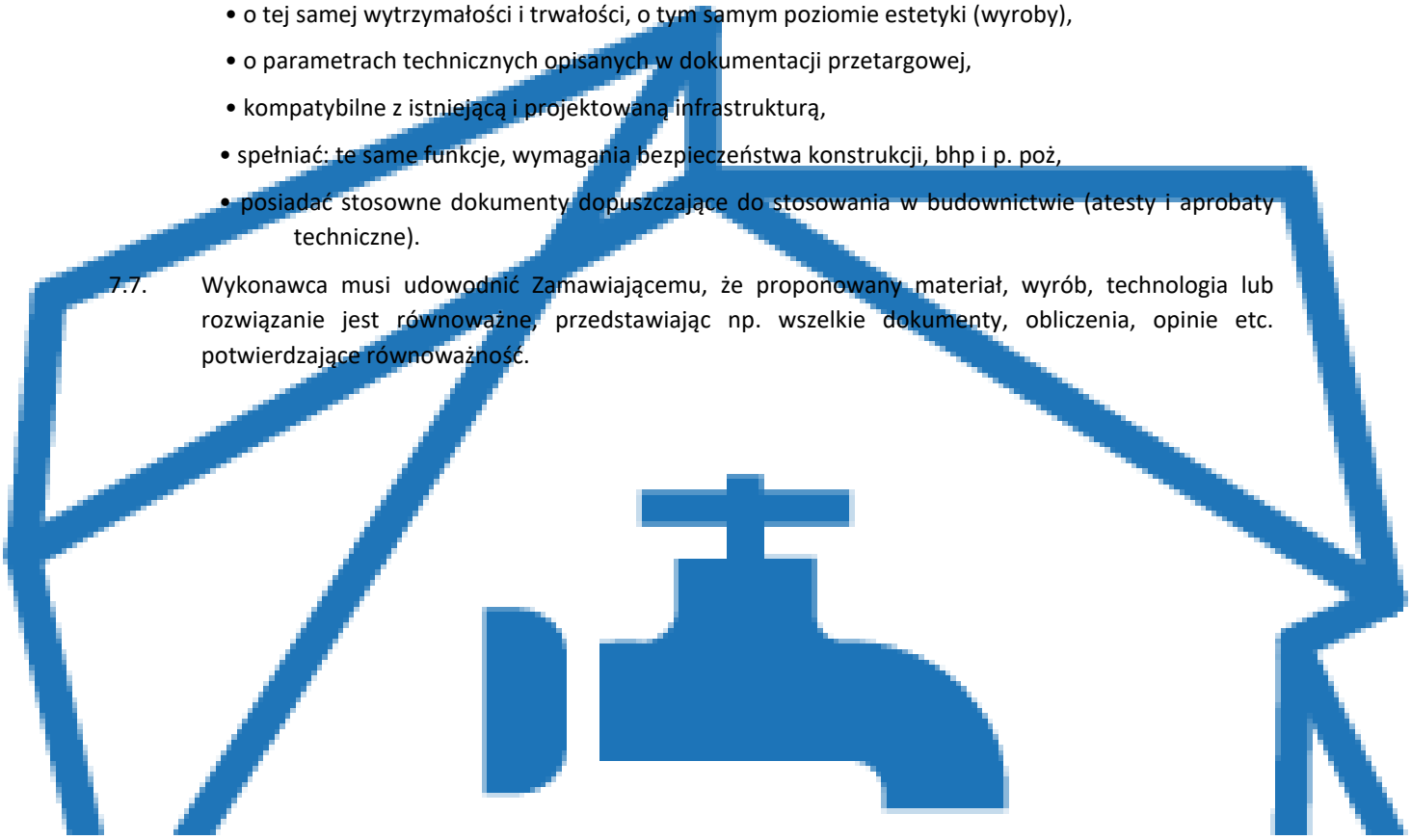
7.4. Wymienione w jakiejkolwiek części OPZ nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

7.5. Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy Zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny".

7.6. Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

7.7. Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.



OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji oprogramowania do uwierzytelniania wieloskładnikowego (MFA) dla sieci IT wraz z wdrożeniem i szkoleniem

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji (subskrypcji) systemu uwierzytelniania wieloskładnikowego (MFA – Multi-Factor Authentication), zwanego dalej „Systemem", dla użytkowników sieci IT Zamawiającego, wraz z wdrożeniem, szkoleniem administratorów oraz wsparciem producenta w okresie obowiązywania licencji.

1.2. Celem zamówienia jest możliwość zabezpieczenia drugim składnikiem uwierzytelniania logowania do stacji roboczych i serwerów Windows (lokalnie i przez RDP), zdalnego dostępu VPN oraz wskazanych aplikacji, zgodnie z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (w brzmieniu nadanym ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252) w zakresie stosowania uwierzytelniania wieloskładnikowego.

1.3. Oferowany System musi istnieć na rynku co najmniej przez okres 3 lat oraz posiadać wsparcie techniczne w języku polskim.

1.4. Producentem Systemu musi być podmiot posiadający siedzibę w Unii Europejskiej.

1.5. Producent Systemu musi posiadać wdrożony system zarządzania bezpieczeństwem informacji, potwierdzony ważnym certyfikatem zgodności z normą ISO/IEC 27001:2023 lub normą równoważną, obejmujący projektowanie i wytwarzanie oprogramowania, bezpieczeństwo informacji oraz ciągłość działania.

1.6. Zakres ilościowy:

Lp.	Element	Ilość	Jedn.
1	Licencja (subskrypcja) Systemu MFA na okres 12 miesięcy od dnia aktywacji, obejmująca wszystkie wymagane funkcje, aktualizacje oraz wsparcie producenta	20	użytkowników
2	Wdrożenie Systemu zgodnie z rozdz. 5	1	usługa
3	Szkolenie administratorów zgodnie z rozdz. 6 (4 godziny, 2 osoby)	1	usługa

1.7. Kody CPV:

48730000-4 – Pakiety oprogramowania zabezpieczającego,
72263000-6 – Usługi wdrażania oprogramowania,
80533100-0 – Usługi szkoleniowe w dziedzinie komputerów.

1.8. Licencja ma być wystawiona na Zamawiającego i umożliwiać zwiększenie liczby chronionych użytkowników w trakcie jej obowiązywania, bez konieczności zmiany Systemu ani ponownego wdrożenia.

2. Opis środowiska Zamawiającego

Wykonawca uwzględni w wdrożeniu następujące środowisko (do uzupełnienia przez Zamawiającego):

Element	Opis
Liczba użytkowników objętych MFA	20
Stacje robocze	system Windows 11 Pro
Serwery chronione MFA (logowanie lokalne/RDP)	Windows Server
Usługa katalogowa	Microsoft Active Directory
Zdalny dostęp VPN	uwierzytelnianie RADIUS/LDAP
Pozostałe systemy do objęcia MFA	panele administracyjne urządzeń sieciowych, SSH do serwerów Linux

Element	Opis
Wirtualizacja (dla komponentów lokalnych)	Proxmox VE / Hyper-V
System SIEM (przekazywanie logów)	
Urządzenia mobilne użytkowników	służbowe

3 Wymagania ogólne

3.1. System musi zawierać polskojęzyczną konsolę administracyjną dostępną z poziomu przeglądarki internetowej umożliwiającą administratorowi jego konfigurację oraz zarządzanie.

3.2 Dostęp do konsoli administracyjnej systemu musi być chroniony uwierzytelnianiem wieloskładnikowym, z możliwością ograniczenia konieczności potwierdzania żądania uwierzytelnienia wieloskładnikowego czynnikiem niepodatnym na ataki phishingowe (np. kluczem sprzętowym typu FIDO2/U2F).

3.3 System musi umożliwiać samodzielną rejestrację i zarządzanie uwierzytelniaczami (tokenami uwierzytelniającymi) przez użytkowników.

3.4 System musi umożliwiać w konsoli administracyjnej rejestrację przez administratora uwierzytelniaczy w postaci sprzętowych kluczy typu FIDO2/U2F dla określonych użytkowników. System musi również umożliwiać zarządzanie zarejestrowanymi uwierzytelniaczami tego typu oraz wyświetlanie szczegółowych informacji na ich temat, w tym adresu IP, z którego dokonano rejestracji, AAGUID, algorytmu COSE oraz licznika podpisów.

3.5 System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez zareagowanie na spersonalizowane powiadomienie wysyłane na urządzenie mobilne użytkownika (mobilne systemy operacyjne iOS, Android oraz Harmony OS).

3.6 System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez wpisanie kodu jednorazowego pochodzącego z dowolnej aplikacji generującej kody jednorazowe zgodnie ze standardem TOTP (RFC 6238). Przykładami takich aplikacji są Microsoft Authenticator oraz Google Authenticator.

3.7 System musi umożliwiać potwierdzenie żądania uwierzytelniania wieloskładnikowego poprzez wpisanie kodu jednorazowego wysłanego na numer telefonu użytkownika w postaci wiadomości SMS.

3.8 System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego poprzez kliknięcie w link wysłany na numer telefonu użytkownika w postaci wiadomości SMS.

3.9 System musi umożliwiać zebranie zgody użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na numer telefonu użytkownika.

3.10 System musi umożliwiać wyświetlanie w konsoli administracyjnej informacji o udzielonej zgodzie od użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na wskazany numer telefonu.

3.11 System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego przy pomocy mobilnej aplikacji uwierzytelniającej, do której dostęp może być zabezpieczony przy pomocy blokady biometrycznej w postaci odcisku palca lub skanu twarzy, jeśli urządzenie mobilne użytkownika posiada taką techniczną możliwość.

3.12 System musi wspierać możliwość potwierdzenia żądania uwierzytelniania wieloskładnikowego poprzez zareagowanie na połączenie telefoniczne nawiązane przez System na stacjonarny lub mobilny numer telefonu użytkownika.

3.13 System musi umożliwiać zakładanie kont administratorów mających dostęp do konsoli administracyjnej wraz z przypisaniem im roli stosownej do zakresu obowiązków danego administratora.

3.14 System musi umożliwiać identyfikowanie użytkowników po aliasach.

3.15 System musi umożliwiać udzielanie dostępu do określonych chronionych rozwiązań informatycznych tylko wybranym grupom użytkowników.

3.16 System musi wygaszać sesję administratora w konsoli administracyjnej w przypadku nieaktywności administratora.

3.17 System musi umożliwiać przeszukiwanie list zarejestrowanych przez użytkowników numerów telefonów oraz kluczy sprzętowych.

3.18 System musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, co najmniej takie jak: grupa, chroniony zasób oraz adres IP użytkownika. System powinien umożliwiać przypisywanie różnych reguł lub polityk indywidualnie do każdej chronionej aplikacji, w zależności od przynależności użytkownika do określonej grupy użytkowników.

3.19 System musi umożliwiać wygenerowanie tymczasowego kodu dostępowego dla wskazanego użytkownika w przypadku niedostępności uwierzytelniacza, np. zagubienia klucza uwierzytelniającego.

3.20 System musi zapewnić logowanie żądań uwierzytelniania użytkowników. System musi umożliwiać pobieranie logów w formacie CSV lub poprzez API.

3.21 System musi zapewnić logowanie zdarzeń związanych z obsługą Systemu (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). System musi umożliwiać pobieranie logów w formacie CSV lub poprzez API.

3.22 System musi posiadać API (pol.: Interfejs Programowania Aplikacji) umożliwiające zarządzanie co najmniej użytkownikami oraz pobieranie logów.

3.23 System musi zapewnić interfejs użytkownika dokonującego uwierzytelniania do chronionych aplikacji w j. polskim.

4 Wymagane Integracje

4.1 System musi zapewniać możliwość uruchomienia uwierzytelniania wieloskładnikowego dla rozwiązań uwierzytelniających użytkowników ze źródeł Active Directory (LDAP, LDAPS) i RADIUS.

4.2 System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows 7 i nowszymi wersjami, oraz do serwerów z systemem operacyjnym Microsoft Windows Server 2008 R2 i nowszymi wersjami. W przypadku braku połączenia z Internetem musi być możliwe wykonanie uwierzytelnienia wieloskładnikowego w postaci jednorazowego hasła (One-Time Password, OTP) i kluczy sprzętowych FIDO oraz kart RFID.

4.3 System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy pomocy sprzętowego klucza zgodnego ze standardem FIDO2 dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows oraz poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server.

4.4 System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy użyciu karty RFID dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows oraz dla logowania poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server.

4.5 System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla technologii: Microsoft Outlook Web App (OWA), Microsoft Remote Desktop Gateway/Web Access/Web Client/Web Feed oraz Microsoft Active Directory Federation Services (AD FS).

4.6 System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń przez protokół Remote Desktop Protocol (RDP).

4.7 System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń SSH do systemów Linux.

4.8 System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do rozwiązań VPN w oparciu o protokoły RADIUS i LDAP.

4.9 System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do urządzeń sieciowych (routery, switche, zapory sieciowe) w oparciu o protokoły RADIUS i LDAP.

4.10 System musi umożliwiać integrację z oprogramowaniem własnym poprzez zastosowanie Software Development Kit (SDK), np. dla oprogramowania .NET, Java, PHP, które umożliwi wykonywanie uwierzytelniania wieloskładnikowego w tym oprogramowaniu.

4.11 System musi umożliwiać jednostronną synchronizację użytkowników ze źródeł Microsoft Active Directory, OpenLDAP oraz Microsoft Entra ID.

4.12 System musi umożliwiać przekazywanie danych do systemu SIEM (Security Information and Event Management), spełniając następujące wymagania:

4.12.1.1 Ciągły eksport dzienników audytowych, uwierzytelniania, zdarzeń związanych z telefonami oraz aktywności.

4.12.2 Obsługa formatów danych JSON oraz Common Event Format (CEF) w wersji 1.

4.12.3 Możliwość konfiguracji wielu niezależnych zadań synchronizacji, z których każde umożliwia wybór jednego lub kilku typów dzienników oraz określenie docelowego systemu SIEM.

5 Wdrożenie

5.1 Oferent jest zobowiązany do dostarczenia oświadczenia Producenta Systemu potwierdzającego, że Oferent jest Autoryzowanym Partnerem Producenta Systemu.

5.2 Oferent jest zobowiązany do dostarczenia oświadczenia Producenta Systemu potwierdzającego, że w przypadku zaprzestania działalności Oferenta (likwidacji, upadłości lub innych przyczyn uniemożliwiających realizację wsparcia technicznego), Producent przejmie zobowiązanie wsparcia technicznego na rzecz Zamawiającego.

6 Wdrożenie

6.1 Wdrożenie obejmuje:

6.1.1 Analizę przedwdrożeniową (warsztat zdalny lub w siedzibie Zamawiającego) i przygotowanie projektu wdrożenia: lista integracji, polityki, grupy, metody uwierzytelniania, procedura awaryjna. Projekt wymaga akceptacji Zamawiającego.

6.1.2 Konfigurację usługi i konsoli administracyjnej, kont administratorów oraz synchronizacji z usługą katalogową.

6.1.3 Instalację i konfigurację serwera proxy RADIUS/LDAP na maszynie wirtualnej udostępnionej przez Zamawiającego.

6.1.4 Instalację i konfigurację agenta MFA na stacjach roboczych i serwerach, w tym przygotowanie pakietu instalacyjnego i dystrybucji (GPO lub ręcznie).

6.1.5 Integrację z VPN/firewallem

6.1.6 Konfigurację polityk zgodnie z projektem, w tym trybu offline i zachowania przy braku łączności (fail-open/fail-closed).

6.1.7 Rejestrację (enrollment) wszystkich 20 użytkowników wraz z ich wsparciem przy instalacji aplikacji mobilnej.

6.1.8 Konfigurację przekazywania logów do systemu SIEM

6.1.9 Przygotowanie procedury awaryjnej (dostęp „break-glass", utrata telefonu, niedostępność usługi) oraz kont awaryjnych.

6.1.10 Testy akceptacyjne według scenariuszy uzgodnionych z Zamawiającym, w tym testy: logowania lokalnego i RDP, VPN, trybu offline, kodów obejścia, polityk sieci/geolokalizacji i zachowania przy braku łączności.

6.1.11 Wdrożenie realizowane będzie etapowo: pilotaż dla grupy 2–3 użytkowników (min. 2 dni robocze), a następnie objęcie pozostałych użytkowników. Prace mogące spowodować przerwę w pracy użytkowników Wykonawca uzgodni z Zamawiającym z wyprzedzeniem co najmniej 2 dni roboczych.

6.1.12 Prace wykonywane będą zdalnie (przez kanał udostępniony i nadzorowany przez Zamawiającego) lub w siedzibie Zamawiającego.

6.1.13 Dokumentacja powykonawcza (w języku polskim, w formie elektronicznej edytowalnej i PDF) obejmuje co najmniej: opis architektury i integracji, konfigurację polityk, wykaz użytkowników i grup, procedurę awaryjną, procedurę dodawania/usuwania użytkownika i wymiany urządzenia oraz protokoły testów. Wykonawca przekaże również krótką instrukcję dla użytkowników (rejestracja i logowanie, maks. 4 strony).

7 Szkolenie

7.1 Wykonawca przeprowadzi szkolenie dla 2 administratorów Zamawiającego w wymiarze 4 godzin zegarowych, w jednym dniu, w terminie uzgodnionym z Zamawiającym, po zakończeniu wdrożenia.

7.2 Formę szkolenia wybiera Zamawiający: stacjonarnie w siedzibie Zamawiającego (koszty dojazdu i pobytu trenera ponosi Wykonawca) albo online na żywo z udziałem prowadzącego. Nie dopuszcza się szkolenia w formie nagrań ani e-learningu.

7.3 Szkolenie prowadzone w języku polskim na wdrożonym Systemie Zamawiającego, przez osobę posiadającą praktyczne doświadczenie we wdrażaniu oferowanego Systemu.

7.4 Ramowy program szkolenia (240 minut):

Moduł	Zakres	Czas
	Architektura Systemu i wdrożone integracje, przepływ uwierzytelniania	30 min
	Konsola administracyjna: użytkownicy, grupy, synchronizacja z AD, role administratorów	45 min
	Polityki: metody, zaufane sieci, zapamiętane urządzenia, geolokalizacja, rejestracja	45 min
	Agent Windows i proxy RADIUS/LDAP: instalacja, konfiguracja, tryb offline, aktualizacje	45 min
	Obsługa zdarzeń: utrata telefonu, kody obejścia, blokada użytkownika, procedura awaryjna	30 min
	Logi, raporty, integracja z SIEM, diagnostyka typowych problemów; pytania	45 min

7.5 Wykonawca przekaże materiały szkoleniowe w języku polskim (elektronicznie) oraz imienne zaświadczenia ukończenia szkolenia.

8. Terminy i odbiór

Etap	Termin
Dostawa i aktywacja licencji	do 3 dni od zawarcia umowy
Projekt wdrożenia (do akceptacji Zamawiającego)	do 2 dni od zawarcia umowy
Zakończenie wdrożenia, testy, dokumentacja	do 7 dni od zawarcia umowy
Szkolenie	do 10 dni od odbioru wdrożenia

8.1. Odbiór dostawy licencji potwierdza protokół odbioru ilościowego. Odbiór wdrożenia potwierdza protokół odbioru końcowego, podpisany po pozytywnym przeprowadzeniu testów akceptacyjnych i przekazaniu dokumentacji. Odbiór szkolenia potwierdza protokół wraz z listą obecności.

8.2. Termin realizacji zamówienia wynosi do 14 od dnia podpisania Umowy.

9. Rozwiązania równoważne

9.1. Opis przedmiotu zamówienia sporządzono za pomocą wymagań funkcjonalnych i wydajnościowych zgodnie z art. 99 ust. 1 ustawy Pzp, bez wskazywania konkretnego producenta. Wszelkie ewentualne odniesienia do norm, znaków towarowych, nazw protokołów lub technologii należy odczytywać z dopiskiem „lub równoważne”.

9.2. Za równoważne uznaje się rozwiązanie spełniające wszystkie wymagania minimalne z rozdz. 3 i 4, w szczególności w zakresie: chronionych systemów (Windows lokalnie i RDP, tryb offline, RADIUS, LDAP, SAML), metod uwierzytelniania (push, TOTP, FIDO2), polityk, logowania zdarzeń oraz lokalizacji przetwarzania danych.

9.3 Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne”.

9.4. Wymienione w jakiejkolwiek części OPZ nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

9.5. Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie

mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy Zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny".

9.6. Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

9.7. Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.

Marcin Łasiński
Elektronicznie podpisany przez Marcin Łasiński
Data: 2026.11.20 15:54:33 +01'00'

