Załącznik nr 3 do SWZ

Szczegółowy opis przedmiotu zamówienia

(Część- Systemy monitorowania i reagowania)

1. SIEM (licencja wieczysta)

Parametr	Opis
Opis systemu	System powinien umożliwiać monitorowanie bezpieczeństwa infrastruktury IT poprzez analizę danych z różnych źródeł, takich jak logi systemowe, zdarzenia sieciowe oraz dane z urządzeń końcowych. Rozwiązanie musi być skalowalne i możliwe do wdrożenia w środowiskach lokalnych, chmurowych oraz hybrydowych. Dopuszcza się realizację wymaganych funkcjonalności poprzez system SIEM oraz współpracujące z nim komponenty bezpieczeństwa dostarczone w ramach zamówienia.
Monitorowanie integralności plików	System powinien umożliwiać wykrywanie zmian w plikach systemowych i konfiguracyjnych, w tym zmian zawartości, uprawnień, właściciela i atrybutów. Wymagana jest możliwość śledzenia użytkownika lub procesu, który dokonał zmiany.
Identyfikacja potencjalnych zagrożeń	System musi analizować dane z logów i plików w celu identyfikacji znanych sygnatur złośliwego oprogramowania oraz podejrzanych zachowań. Powinien wspierać integrację z zewnętrznymi źródłami informacji o zagrożeniach.
Ocena konfiguracji bezpieczeństwa	Rozwiązanie powinno umożliwiać automatyczne skanowanie systemów pod kątem zgodności z politykami bezpieczeństwa, standardami branżowymi i regulacjami. Wymagana jest możliwość tworzenia własnych polityk oceny.
Reakcja na incydenty	System musi umożliwiać automatyczne wykonywanie działań naprawczych w odpowiedzi na wykryte zagrożenia, takich jak blokowanie adresów IP, zatrzymywanie procesów czy modyfikacja reguł zapory.
Zbieranie i analiza logów	System powinien zbierać logi z różnych źródeł (systemy operacyjne, aplikacje, urządzenia sieciowe) i analizować je w czasie rzeczywistym przy użyciu reguł detekcji.
Wykrywanie luk w zabezpieczeniach	Rozwiązanie musi identyfikować znane podatności w zainstalowanym oprogramowaniu poprzez porównanie z aktualnymi bazami danych podatności.
Inwentaryzacja zasobów	System powinien automatycznie zbierać informacje o zainstalowanym oprogramowaniu, sprzęcie, usługach i konfiguracjach systemowych.
Monitorowanie kontenerów i środowisk wirtualnych	Wymagana jest możliwość monitorowania środowisk kontenerowych i maszyn wirtualnych, w tym ich konfiguracji, uruchamianych procesów i komunikacji sieciowej.
Monitorowanie bezagentowe	System powinien umożliwiać zbieranie danych z urządzeń, na których nie można zainstalować agenta, np. poprzez protokoły zdalnego dostępu.
Korelacja zdarzeń i reguły detekcji	Rozwiązanie musi umożliwiać tworzenie i modyfikację reguł detekcji oraz korelację zdarzeń z wielu źródeł w celu identyfikacji złożonych zagrożeń.
Integracja z systemami zewnętrznymi	System powinien wspierać integrację z platformami chmurowymi, narzędziami do zarządzania incydentami, systemami zarządzania tożsamością oraz źródłami informacji o zagrożeniach.
Wizualizacja danych i dashboard	Wymagana jest możliwość tworzenia interaktywnych pulpitów nawigacyjnych, wykresów, map zagrożeń oraz przeglądania alertów w czasie rzeczywistym.
Zarządzanie użytkownikami i dostępem	System powinien wspierać integrację z usługami katalogowymi oraz umożliwiać zarządzanie rolami i uprawnieniami użytkowników.
Zarządzanie agentami i konfiguracją	Rozwiązanie musi umożliwiać centralne zarządzanie komponentami zbierającymi dane, ich konfiguracją, aktualizacją oraz monitorowaniem stanu.
Obsługa wielu systemów operacyjnych	System powinien wspierać monitorowanie systemów Windows, Linux, macOS oraz urządzeń sieciowych.
Zgodność z regulacjami	Rozwiązanie musi wspierać zgodność z normami takimi jak RODO, PCI DSS, ISO 27001, NIST, HIPAA poprzez gotowe szablony i raporty lub otwarty mechanizm tworzenia raportów (kreator raportów)

Raportowanie i alertowanie	System powinien umożliwiać generowanie raportów cyklicznych oraz alertowanie w czasie rzeczywistym z możliwością dostosowania progów i kanałów powiadomień.
Zdalne wykonywanie poleceń i skryptów	System powinien umożliwiać zdalne uruchamianie poleceń lub skryptów na urządzeniach końcowych za pośrednictwem komponentu agenta. Funkcjonalność ta musi być dostępna z poziomu centralnego interfejsu zarządzania i umożliwiać wykonywanie operacji administracyjnych, diagnostycznych lub naprawczych. Zamawiający dopuszcza realizację funkcjonalności poprzez bezpośrednie wykonywanie poleceń ad-hoc lub poprzez centralnie zarządzane skrypty, zadania, reguły i mechanizmy automatycznej reakcji. Funkcjonalność musi umożliwiać operatorowi zainicjowanie działania na wskazanym urządzeniu końcowym bez konieczności oczekiwania na cykliczną synchronizację polityk lub konfiguracji.
Obsługa wielu języków skryptowych	Rozwiązanie powinno wspierać wykonywanie skryptów w różnych językach, takich jak Bash, PowerShell, Python lub inne dostępne lokalnie na monitorowanym systemie.
Warunkowe wykonywanie zadań	System musi umożliwiać definiowanie warunków, które muszą zostać spełnione przed wykonaniem skryptu (np. system operacyjny, adres IP, stan usługi).
Bezpieczeństwo i kontrola dostępu	Wymagana jest możliwość ograniczenia dostępu do funkcji zdalnego wykonywania poleceń na podstawie ról użytkowników oraz prowadzenie pełnej rejestracji działań (logowanie kto, kiedy i co wykonał).
Zbieranie wyników wykonania	System powinien umożliwiać zbieranie wyników wykonanych poleceń i ich prezentację w interfejsie zarządzania, z możliwością dalszej analizy i korelacji.
Automatyzacja reakcji	Funkcjonalność powinna być zintegrowana z mechanizmem automatycznej reakcji na incydenty, umożliwiając uruchamianie skryptów w odpowiedzi na wykryte zagrożenia lub zdarzenia.
Obsługa harmonogramów i opóźnień	System powinien umożliwiać planowanie zadań do wykonania w określonym czasie lub z opóźnieniem, a także ich cykliczne uruchamianie.
Obsługa wielu systemów operacyjnych	Funkcja musi działać na różnych platformach systemowych, w tym systemach typu Unix/Linux, Windows oraz macOS.
Ograniczenie środowiska wykonania	Wymagana jest możliwość ograniczenia środowiska wykonania (np. zmienne środowiskowe, katalog roboczy, uprawnienia), aby zwiększyć bezpieczeństwo operacji.
Wsparcie techniczne	Dostawca musi zapewnić dostęp do wsparcia technicznego na okres min. 12 miesięcy, obejmujący pomoc w konfiguracji oraz pomoc w rozwiązywaniu usterek technicznych
Kanały kontaktu	Wsparcie techniczne powinno być dostępne przez e-mail, telefon oraz system zgłoszeniowy.
Język wsparcia	Wymagane jest wsparcie techniczne w języku polskim lub angielskim
Dostęp do dokumentacji	Klient musi mieć dostęp do pełnej dokumentacji technicznej i użytkowej w języku polskim, obejmującej instrukcje instalacji, konfiguracji, tworzenia reguł, integracji oraz zarządzania incydentami.
Realizacja techniczna	Zamawiający dopuszcza realizację wymaganych funkcjonalności za pomocą zestawu współpracujących komponentów lub modułów, pod warunkiem zapewnienia jednolitego procesu zarządzania.

2. System monitorowania infrastruktury (licencja wieczysta)

Parametr	Opis
Ogólne Funkcje	• udostępnienie widoków bazodanowych dla wszystkich modułów oprogramowania • filtr dla grup inteligentnych: Użytkownik należy/nie należy do grupy • filtr dla map inteligentnych: BitLocker -> Wolumin systemowy
	• powiadomienia (pulpitowe, e-mailowe, SMS-owe) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.) • powiadomienie o alarmach wysyłane za pośrednictwem popularnych komunikatorów biznesowych (np. Microsoft Teams, Slack lub równoważne) oraz za pośrednictwem usług SMS poprzez API dostawcy zewnętrznego • obsługa OAuth 2.0 w konfiguracji skrzynki e-mail dla alarmów i 2FA • 2FA uwierzytelnianie dwuskładnikowe w logowaniu do konsoli (e-mail i SMS) • obsługa OAuth 2.0 w konfiguracji skrzynek e-mail w HelpDesk • integracja z bramkami SMS oraz urządzeniami monitoringu środowiskowego lub równoważnymi • jednoczesna praca wielu administratorów, dziennik dostępu administratorów • uwierzytelnianie wieloskładnikowe i zwiększone wymogi dla haseł • szyfrowana synchronizacja z Active Directory z wykorzystaniem LDAPS (Secure LDAP) • Agent na Windows • ochrona Agenta przed usunięciem

	• pakiet narzędzi diagnostycznych • alarmy zdarzenie-akcja • zarządzanie hierarchią użytkowników (w tym import z AD) • raporty dla użytkowników, urządzeń, oddziałów, map sieci lub całego atlasu • zarządzanie uprawnieniami wielu administratorów • zarządzanie grupami (tworzenie, przypisywanie użytkowników) • menu kontekstowe z możliwością definiowania własnych narzędzi • dziennik dostępu administratorów: wysyłanie zdarzeń do zewnętrznego kolektora Syslog • globalne wyszukiwanie obiektów w konsoli zarządzania • logowanie w konsoli deinstalacji Agenta • dodawanie awatarów i pobieranie ich z Active Directory
Funkcje sieciowe	• skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP • interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne • serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.) • liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp. • działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń • liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
	• monitorowanie i zarządzanie maszynami wirtualnymi VMware oraz Hyper-V • kompilator plików MIB • obsługa pułapek SNMP • routery i switche: mapowanie portów; informacja, do którego przełącznika jest podłączone urządzenie • obsługa komunikatów Syslog • obsługa szyfrowania AES, DES i 3DES dla protokołu SNMPv3 • możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca)
Funkcje dotyczące zasobów	• szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu • możliwość tworzenia własnych relacji między dowolnymi zasobami i dowolnego opisywania ich • widok zasobów, aplikacji, dokumentów, licencji dla poszczególnych użytkowników lub osobny widok według zasobów przypisanych do urządzeń • Software Asset Management rozbudowany system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji • rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji • informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej • szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej • alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych • aplikacja mobilna do wsparcia procesów inwentaryzacyjnych dla systemu Android umożliwiający wyszukiwanie, dodawanie i edycję zasobów, dodawanie czynności serwisowych, spis z natury na bazie kodów kreskowych, kodów QR, generowanie etykiet w konsoli • IT Asset Management zarządzanie wszelkimi zasobami, za które odpowiada dział IT • jednoczesne przypisywanie dokumentu do wielu zasobów • uprawnienia dostępu administratorów do typów zasobów, licencji i dokumentów w ramach oddziałów • masowa edycja atrybutów zasobów, np. statusu. • rozliczanie dowolnego typu licencji, w tym modelowanie licencji chmurowych • audyt inwentaryzacji sprzętu i oprogramowania • wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach • manager plików z możliwością usuwania plików użytkownika
	• zarządzanie instalacjami / dezinstalacjami oprogramowania przez menedżera pakietów MSI • możliwość archiwizacji i porównywania audytów • automatyczne numerowanie dodawanych zasobów oraz dokumentów wg. zdefiniowanego wzorca numeracji • historia użycia konkretnej licencji oprogramowania • odczyt danych S.M.A.R.T. z dysków NVMe oraz SATA • zmiana wielkości kodu QR na wydrukowanej etykiecie
Funkcje dotyczące użytkowników	• blokowanie uruchamianych aplikacji (na podstawie lokalizacji pliku .EXE) • rejestrowanie aktywności stacji roboczej obejmujące czas logowania, wylogowania oraz okresy aktywności i nieaktywności systemu • użytkowane aplikacje (aktywnie i nieaktywnie) • odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)

	• audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków • blokowanie stron WWW • rejestr naruszeń blokad agregujący informacje o próbie dostępu do blokowanych stron WWW, uruchamianiu zakazanych aplikacji oraz pobieraniu plików z niedozwolonymi rozszerzeniami • możliwość korzystania z zewnętrznych list blokowania stron, w tym z listą ostrzeżeń CERT.PL • zgodność z RODO przyporządkowanie konfiguracji, uprawnień i dostępów do konkretnego użytkownika niezależnie od urządzenia • pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa • statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) • dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad • możliwość wykrywania nietypowych lub anormalnych wzorców aktywności na stacjach roboczych, mogących wskazywać na obejście polityk bezpieczeństwa lub automatyzację działań użytkownika • centralna konfiguracja: ustawienie reguł dla całej sieci oraz dla grup użytkowników Active Directory • monitorowanie odwiedzanych stron WWW w popularnych przeglądarkach internetowych, tym co najmniej Google Chrome, Microsoft Edge, Mozilla Firefox oraz Opera
Funkcje dotyczące plików	• audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych
	• monitorowanie operacji na plikach w katalogach na dysku systemowym • monitorowanie operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez Agenta np. macierze Synology, Qnap itp. • zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników • alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym oraz na dyskach lokalnych • automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa • integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania • integracja z Windows BitLocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów • możliwość zdalnego szyfrowania dysków za pomocą funkcji BitLocker • integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych • informacje o urządzeniach podłączonych do danego komputera • lista wszystkich urządzeń podłączonych do komputerów w sieci • centralna konfiguracja: ustawienie regułdla całej sieci oraz grup i użytkowników Active Directory • integracja bazy użytkowników i grup z Active Directory • atrybut „nośnik zaufany” • możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB) • prezentacja aktualnych ustawień polityk bezpieczeństwa, uprawnień oraz konfiguracji przypisanych do użytkownika • wykrywanie oprogramowania antywirusowego innego niż Windows Defender
Sposób realizacji	Dopuszcza się realizację wymaganych funkcjonalności za pomocą jednego produktu lub zestawu współpracujących komponentów pochodzących od jednego lub wielu producentów.

3. NAC (licencja wieczysta)

Parametr	Opis

Podstawowe funkcjonalności wymagania	1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych i 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 niewymagających obsługi dodatkowych wtyczek. 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 300 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 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) co najmniej tyle samo co licencja 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. Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.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 uwierzytelnienia gościnnego. 12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP. 13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, 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 ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. 15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. OIDC/oAuth2, SAML/Kerberos, Radius, LDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC). 16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. 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 nie połączonych relacjami zaufania. 19. System musi mieć możliwość obsługę 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, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, 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, na którym dostępny jest podgląd 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. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych 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.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji 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 2 z wymienionych:
Facebook, Google, LinkedIn, Microsoft.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze 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 dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań.

	51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. 52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, 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 określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. 54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. 55. System musi posiadać dedykowanego agenta min dla systemu Windows, w celu profilowania urządzeń końcowych. 56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. 57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. Microsoft Intune, Google Workspace). 58. Obsługa uwierzytelniania wieloskładnikowego (OTP) dla popularnych rozwiązań VPN i zdalnego dostępu, w tym rozwiązań klasy Fortinet, Cisco, Palo Alto, OpenVPN lub równoważnych. 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 włączony jest firewall • Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur • Czy jest włączone 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 oraz typu wartości: Number, String, Version 60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. 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 dla systemów co najmniej: – Microsoft Windows – Mac OS – 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, komunikację z Microsoft Active Directory. 65. Zamawiający dopuszcza realizację wymaganych funkcjonalności za pomocą zestawu współpracujących komponentów lub modułów, pod warunkiem zapewnienia jednolitego procesu zarządzania.
Mechanizmy uwierzytelniania	1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. 2. System musi obsługiwać uwierzytelnianie co najmniej w oparciu o następujące protokoły: • IEEE 802.1X, • EAP-TLS, • PEAP, • PAP, • CHAP, • MS-CHAPv2, • MAC Authentication Bypass (MAB),

- Captive Portal

4. Organizacja realizacji zamówienia

a) Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
b) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
c) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w SWZ i nie są z nimi sprzeczne.
d) W niniejszym dokumencie opisano wymagania minimalne.
e) W przypadku oferowania oprogramowania open source, jest to dopuszczalne pod warunkiem spełnienia warunku zapewnienia min. rocznego płatnego okresu wsparcia
f) Wszelkie nazwy własne technologii, standardów, producentów lub produktów użyte w dokumentacji należy interpretować jako przykładowe, o ile nie wynikają z wymagań kompatybilności z istniejącą infrastrukturą Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne spełniające wymagania funkcjonalne, techniczne, administracyjne, integracyjne i licencyjne określone w niniejszym dokumencie.
g) Za rozwiązanie równoważne uznaje się rozwiązanie realizujące wymagane funkcjonalności, bezpieczeństwo, integrację i sposób eksploatacji określone w niniejszym dokumencie, niezależnie od zastosowanej architektury technicznej, nazewnictwa funkcji lub podziału funkcjonalności pomiędzy moduły i komponenty.
h) W przypadku rozwiązań równoważnych obowiązek wykazania równoważności spoczywa na Wykonawcy.