

ZP.271.256.2025

Załącznik nr 2 do SWZ

Spis treści

Opis Przedmiotu Zamówienia	3
Słownik	3
1. Organizacja realizacji zamówienia	7
2. Przeprowadzenie szkoleń	8
2.1. Wymagania ogólne dla szkolenia	8
2.2. Wymagania szczegółowe dla szkoleń	9
3. Wdrożenie	9
4. Warunki równoważności	9
5. Specyfikacja przedmiotu zamówienia	10
5.1. Opis wymagań wspólnych dla producentów i produktów dostarczanych w ramach przedmiotu zamówienia	10
5.1.1. Charakterystyka firmy i produktu	10
5.1.2. Charakterystyka techniczna produktu	11
5.1.3. Wsparcie, aktualizacje i rozwój	11
5.2. Wymagania dla systemu Network Access Control	13
5.2.1. Podstawowe funkcjonalności oraz wymagania	13
5.2.2. Mechanizmy uwierzytelniania	23
5.2.3. Obsługa serwerów certyfikatów CA	26
5.2.4. Obsługa serwerów DHCP	27
5.2.5. Obsługa serwerów TACACS+	29
5.2.6. Raportowanie i monitoring	30
5.2.7. Alarmy	33
5.2.8. Wymagania dotyczące wdrożenia i harmonogram ramowy	34
5.2.9. Licencja i wsparcie techniczne producenta oprogramowania	36
5.2.10. Szkolenia	37
5.3. Wymagania dla systemu Privilege Access Management	39
5.3.1. Monitorowanie Aktywności Użytkowników	39
5.3.2. Licencjonowanie	43
5.3.3. Obsługiwane platformy	44
5.3.4. Wdrożenie	45
5.3.5. Zarządzanie dostępem i alertami	48
5.3.6. Produktywność i Raportowanie	51
5.3.7. Zarządzanie hasłami	53
5.3.8. Szkolenia	55
5.4. Wymagania dla Web Application Firewall (SaaS)	56
5.4.1. Licencjonowanie	56
5.4.2. Zabezpieczenia aplikacji internetowych	57
5.4.3. Optymalizacja wydajności aplikacji internetowych	59
5.4.4. Ochrona przed botami	61
5.4.5. Optymalizacja SEO i prędkości ładowania strony	62
5.4.6. Szkolenia	63
5.5. Wymagania dla System Information and Event Management	65

5.5.1.	Zarządzanie logami i analiza zdarzeń	65
5.5.2.	Zarządzanie incydentami i odpowiedź na zagrożenia	67
5.5.3.	Automatyzacja i zarządzanie regułami	68
5.5.4.	Rozszerzone funkcje analizy zagrożeń i automatyzacji	70
5.5.5.	Rozszerzone funkcje raportowania i monitorowania zgodności	72
5.5.6.	Rozszerzone funkcje monitorowania operacyjnego i automatyzacji operacji	74
5.5.7.	Szkolenia	76
5.6.	Autoryzowane szkolenie Fortigate Administrator	77
6.	Zamówienie jest przeznaczone do użytku osób fizycznych, zatem Zamawiający uwzględnił w opisie przedmiotu zamówienia wymagania w zakresie dostępności osób z niepełnosprawnością.	79



Opis Przedmiotu Zamówienia

Słownik

L.P	Pojęcie	Opis
	Zamawiający	Gmina Dobrzeń Wielki
	SIEM (Security Information and Event Management)	Technologia zarządzania informacjami i zdarzeniami bezpieczeństwa, która zbiera, analizuje i koreluje dane z różnych źródeł w infrastrukturze IT organizacji, takich jak systemy operacyjne, aplikacje, urządzenia sieciowe oraz systemy bezpieczeństwa. SIEM umożliwia identyfikację potencjalnych zagrożeń i anomalii w czasie rzeczywistym, generując alerty oraz dostarczając narzędzia do analiz i raportowania w zakresie bezpieczeństwa. Dzięki centralizacji logów i zaawansowanej analizie, SIEM wspiera zespoły bezpieczeństwa w szybkim wykrywaniu incydentów oraz zarządzaniu zgodnością z regulacjami.
	WAF (Web Application Firewall)	System ochrony aplikacji webowych przed zagrożeniami online, który monitoruje, filtruje i blokuje złośliwy ruch HTTP, zanim dotrze on do aplikacji. System ten korzysta z zaawansowanych reguł i technologii, takich jak wykrywanie i zapobieganie atakom DDoS na poziomie aplikacji, automatyczne blokowanie botów oraz filtrowanie ruchu na podstawie analizy reputacji IP. Dodatkowo, WAF oferuje wsparcie dla dostosowywania reguł bezpieczeństwa w czasie rzeczywistym, a także umożliwia ochronę przed popularnymi atakami na aplikacje webowe, takimi jak SQL Injection, Cross-Site Scripting (XSS) oraz inne podatności z listy OWASP.
	PAM (Privileged Access Management)	System zarządzania dostępem uprzywilejowanym, który umożliwia kontrolowanie i monitorowanie działań użytkowników z dostępem do krytycznych zasobów organizacji. Rozwiązanie to zapewnia pełny wgląd w sesje użytkowników uprzywilejowanych, oferując funkcje takie jak rejestrowanie i nagrywanie sesji w czasie rzeczywistym oraz możliwość analizy aktywności po fakcie. Dodatkowo PAM oferuje szczegółową kontrolę uprawnień oraz

		możliwość natychmiastowego blokowania podejrzanych działań, co wzmacnia bezpieczeństwo infrastruktury IT poprzez ścisły nadzór nad kontami o wysokim poziomie dostępu.
	NAC (Network Access Control)	Rozwiązanie do zarządzania dostępem do sieci, które zapewnia kontrolę nad urządzeniami łączącymi się z siecią oraz monitoruje ich zachowanie w czasie rzeczywistym. System ten umożliwia pełną widoczność urządzeń, automatycznie identyfikuje i klasyfikuje każde nowe urządzenie, a także stosuje zasady dostępu na podstawie profili użytkowników i typów urządzeń. Ponadto NAC oferuje zaawansowane funkcje reagowania, takie jak dynamiczne przydzielanie dostępu, izolowanie zagrożonych urządzeń oraz zdalne blokowanie nieautoryzowanych połączeń, co wspiera bezpieczeństwo sieci poprzez skuteczne zarządzanie urządzeniami i zgodnością polityk bezpieczeństwa.
	Środowisko aplikacyjne	<p>Zintegrowane środowisko, które obejmuje wszystkie zasoby, narzędzia, oprogramowanie, usługi i konfiguracje niezbędne do uruchamiania, testowania, wdrażania oraz utrzymania aplikacji w ramach infrastruktury IT. Jest to ekosystem, w którym aplikacja funkcjonuje, obejmujący zarówno komponenty sprzętowe, jak i programowe, które wspierają działanie i rozwój aplikacji.</p> <p>Kluczowe Elementy Środowiska Aplikacyjnego:</p> <p>Sprzęt (Hardware):</p> <p>Serwery: Maszyny fizyczne lub wirtualne, na których uruchamiane są aplikacje.</p> <p>Pamięć Masowa: Dyski twarde, SSD, systemy SAN/NAS do przechowywania danych.</p> <p>Sieć: Urządzenia sieciowe, takie jak routery, przełączniki, firewalle, które umożliwiają komunikację między komponentami systemu.</p> <p>Oprogramowanie (Software):</p>

System Operacyjny: Podstawowe oprogramowanie, które zarządza zasobami sprzętowymi i dostarcza usług dla aplikacji (np. Windows, Linux).

Serwer Aplikacji: Oprogramowanie, które uruchamia aplikacje i zarządza ich działaniem (np. Apache Tomcat, Microsoft IIS).

Baza Danych: System zarządzania bazą danych (DBMS) używany do przechowywania i zarządzania danymi aplikacji (np. MySQL, PostgreSQL, Oracle).

Narzędzia Programistyczne: IDE, frameworki, biblioteki i inne narzędzia używane do tworzenia i testowania aplikacji (np. Eclipse, Visual Studio, Spring, Django).

Usługi i Infrastruktura (Services and Infrastructure):

Chmura: Usługi chmurowe, które oferują skalowalne zasoby obliczeniowe i pamięciowe (np. AWS, Microsoft Azure, Google Cloud Platform).

Usługi Wspomagające: Usługi takie jak serwery DNS, serwery proxy, usługi cache'owania (np. Redis, Memcached).

Konfiguracja i Zarządzanie (Configuration and Management):

Konfiguracja Systemu: Ustawienia i parametry konfiguracyjne aplikacji i jej środowiska.

Monitorowanie i Logowanie: Systemy monitorowania wydajności i dostępności aplikacji, oraz logowania błędów i zdarzeń (np. Nagios, Prometheus, ELK Stack).

Bezpieczeństwo (Security):

Kontrola Dostępu: Mechanizmy autoryzacji i uwierzytelniania użytkowników.

Ochrona Danych: Szyfrowanie danych, backupy, polityki zarządzania danymi.

		<p>Testy Bezpieczeństwa: Regularne audyty i testy penetracyjne w celu identyfikacji i eliminacji podatności.</p> <p>Dla aplikacji webowej, środowisko aplikacyjne może obejmować:</p> <p>Serwer WWW: Apache HTTP Server lub Nginx.</p> <p>System Operacyjny: Ubuntu Linux.</p> <p>Baza Danych: MySQL lub PostgreSQL.</p> <p>Język Programowania: Python z frameworkiem Django.</p> <p>Usługi Chmurowe: AWS EC2 dla serwerów aplikacji, S3 dla przechowywania danych, RDS dla bazy danych.</p> <p>Narzędzia Monitorujące: Prometheus dla monitorowania wydajności, Grafana dla wizualizacji danych.</p> <p>Mechanizmy Bezpieczeństwa: Certyfikaty SSL/TLS dla zabezpieczenia komunikacji, usługi WAF (Web Application Firewall) dla ochrony przed atakami.</p>
	2700X	<p>Zamawiający, ilekroć mowa o 27001 ma na myśli normy:</p> <p>PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania,</p> <p>PN-EN ISO/IEC 27002:2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji.</p>
	RODO	<p>RODO (Rozporządzenie o Ochronie Danych Osobowych), czyli Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., to akt prawny regulujący zasady przetwarzania danych osobowych osób fizycznych w Unii Europejskiej</p>

	Wdrożenie	Proces instalacji, konfiguracji oraz uruchomienia aplikacji lub systemu w środowisku produkcyjnym, aby spełniał on określone wymagania użytkowników i organizacji oraz zadań samej aplikacji. Proces wdrożenia obejmuje kroki, co najmniej następujące kroki, przygotowanie infrastruktury, migrację danych, testowanie funkcjonalności oraz szkolenie użytkowników końcowych. Celem wdrożenia jest zapewnienie, że oprogramowanie działa poprawnie i efektywnie w docelowym środowisku, wspierając działalność operacyjną oraz osiągnięcie celów organizacji.
	Integracja	Proces łączenia różnych systemów lub aplikacji w taki sposób, aby mogły one współpracować i wymieniać dane w ramach jednej, spójnej platformy. Integracja obejmuje projektowanie i wdrażanie interfejsów oraz protokołów komunikacyjnych, które umożliwiają automatyczny przepływ informacji pomiędzy systemami, minimalizując konieczność ręcznego wprowadzania danych. Celem integracji oprogramowania jest zwiększenie efektywności operacyjnej, poprawa dostępności informacji oraz umożliwienie bardziej złożonych analiz i raportowania poprzez płynny przepływ danych między różnymi narzędziami.

1. Organizacja realizacji zamówienia

- 1) 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.
- 2) Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiającego nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- 3) Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- 4) Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby

- Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- 5) Jakikolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
 - 6) Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
 - 7) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
 - 8) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
 - 9) Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
 - 10) Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.

2. Przeprowadzenie szkoleń

Wszystkie szkolenia winny być przeprowadzone dla Urząd Gminy w Dobrzenu Wielkim.

2.1. Wymagania ogólne dla szkolenia

- 2.1.1. Szkolenie powinno odbyć się w siedzibie Zamawiającego ale Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń i być gotowym do organizacji szkolenia online.
- 2.1.2. Zamawiający udostępni bezpłatnie pomieszczenie wyposażone w rzutnik oraz dostęp do Internetu, na potrzeby szkolenia stacjonarnego.
- 2.1.3. Każde szkolenie powinno trwać od 3 do 6 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia.
- 2.1.4. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 8.30 – 15.00 w siedzibie Zamawiającego albo zdalnie.
- 2.1.5. W celu maksymalizacji czasu nie przewiduje się przerw podczas szkolenia.
- 2.1.6. W przypadku błędów albo braku możliwości uruchomienia szkolenia z uwagi na usterki techniczne Wykonawca zobowiązany jest do naprawy ww. szkolenia.
- 2.1.7. Szkolenie winno być uzupełnione o test wiedzy gwarantujący możliwość weryfikacji umiejętności kursantów. Test wiedzy musi automatyzować zbieranie i ocenę wyników.
- 2.1.8. W ramach organizacji szkoleń Wykonawca zapewni:
 - 2.1.8.1. Materiały szkoleniowe dla każdego uczestnika szkolenia w postaci elektronicznej, które Zamawiający będzie mógł wykorzystać nieodpłatnie i wydrukować dla każdego uczestnika. Materiały muszą zawierać szczegółowe informacje, które będą omawiane podczas szkolenia.
 - 2.1.8.2. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

2.2. Wymagania szczegółowe dla szkoleń

- 2.2.1. Szkolenia mają dotyczyć instalacji, konfiguracji oraz poprawności działania każdego rozwiązania stanowiącego przedmiot projektu.
- 2.2.2. Szkolenia mają zawierać moduł dedykowany dla zrozumienia korzyści, które niosą informacje dostarczane przez każde z narzędzi.
- 2.2.3. Szkolenie ma zawierać moduł dedykowany rozwiązywaniu problemów z wdrażanym rozwiązaniem.
- 2.2.4. Szkolenie ma zawierać moduł dotyczący zarządzania incydem wynikającym z wdrażanego rozwiązania.

3. Wdrożenie

- 3.1.1. Każdy z systemów stanowiący przedmiot dostawy winien zostać wdrożony w sposób umożliwiający prawidłowe funkcjonowanie bez negatywnego wpływu na środowisko Zamawiającego.
- 3.1.2. W przypadku dostawy licencji Wykonawca wdroży minimalnie 20% licencji oraz skonfiguruje całość rozwiązania by działało prawidłowo.
- 3.1.3. W przypadku dostawy rozwiązania opierającego się o serwer Wykonawca wdroży je w całości na serwerze oraz w 20% na urządzeniach/użytkownikach objętych wdrożeniem.
- 3.1.4. Wdrożenie ma odbywać się wraz z Zamawiającym co oznacza, że Wykonawca będzie prowadził prace bezpośrednio w obecności Zamawiającego.

4. Warunki równoważności

- 4.1.1. Wszędzie, gdzie użyto nazw własnych produktów oraz nazwy certyfikatów Zamawiający stosuje zasadę równoważności która określa przedmiot zamówienia o cechach technicznych, jakościowych lub funkcjonalnych takich samych lub zbliżonych do tych, które zawiera zakres równoważności wskazany w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
- 4.1.2. W przypadku wątpliwości Zamawiający oczekuje pytań ze strony Wykonawcy, które będą zawierały odniesienie do rozwiązania lub certyfikatu uważanego za równoważny przez Wykonawcę z oczekiwanym przez Zamawiającego.
- 4.1.3. Zamawiający dopuści rozwiązania równoważne o ile zagwarantują one takie same parametry jakościowe dla zaoferowanych usług jak oczekiwane przez Zamawiającego.

Jako certyfikat równoważny do certyfikatu Togaf 9 Zamawiający uzna certyfikat, który:

- Dotyczy zakresu architektury,
- Metoda Rozwoju Architektury (ADM) i jej produkty, w tym architektura biznesowa, danych, aplikacji i techniczna,
- Kontinuum Korporacyjne,
- Ład Architektoniczny,
- Pryncypia Architektoniczne i ich tworzenie,
- Widoki i architektoniczne punkty widzenia,

- Zarządzanie wymaganiami z użyciem scenariuszy biznesowych,
- Ocena poziomu dojrzałości architektury,
- Ramy umiejętności architektonicznych,
- Partycjonowanie i segmentacja architektury,
- Ramy zawartości i metamodel,
- Planowanie rozwoju oparte na potencjale/zdolnościach,
- Ocena gotowości biznesu do transformacji,
- Usystematyzowane podejście do zarządzania zmianą organizacyjną na bazie modeli architektonicznych do tworzenia architektur bezpieczeństwa,
- Repozytorium architektoniczne;

5. Specyfikacja przedmiotu zamówienia

5.1. Opis wymagań wspólnych dla producentów i produktów dostarczanych w ramach przedmiotu zamówienia

5.1.1. Charakterystyka firmy i produktu

Lp.	Wymaganie	Wyjaśnienie
1.	Minimum 5 lat obecności produktu na rynku	Produkt powinien być dostępny na rynku co najmniej 5 lat, co potwierdza jego dojrzałość i weryfikację przez użytkowników.
2.	Regularne aktualizacje produktu	Produkt powinien być regularnie aktualizowany (minimum raz na kwartał), aby zapewniać bezpieczeństwo i wprowadzać nowe funkcje.
3.	Wsparcie techniczne	Firma powinna oferować wsparcie techniczne, aby zapewnić użytkownikom pomoc w przypadku awarii lub problemów z produktem.
4.	Sieć partnerów wdrożeniowych	Producent powinien posiadać rozbudowaną sieć certyfikowanych partnerów wdrożeniowych na całym świecie, aby wspierać procesy implementacji.
5.	Dokumentacja i zasoby szkoleniowe	Firma powinna zapewniać szczegółową dokumentację oraz zasoby edukacyjne dla administratorów i użytkowników końcowych.

Lp.	Wymaganie	Wyjaśnienie
6.	Bezpieczeństwo potwierdzone przez audyty	Producent powinien przeprowadzać regularne audyty bezpieczeństwa, które potwierdzają zgodność z najnowszymi standardami bezpieczeństwa.

5.1.2. Charakterystyka techniczna produktu

Lp.	Wymaganie	Wyjaśnienie
1.	Integracja z innymi systemami bezpieczeństwa	Produkt powinien umożliwiać integrację z innymi narzędziami bezpieczeństwa (np. SIEM, endpoint), aby wspierać kompleksową ochronę.
2.	Skalowalność	Produkt powinien być skalowalny, aby obsługiwać zarówno małe, jak i duże organizacje, dostosowując się do liczby użytkowników i zasobów.
3.	Wsparcie dla środowisk wirtualnych	Produkt powinien obsługiwać środowiska wirtualne, takie jak VMware, Hyper-V, aby wspierać wdrożenia w nowoczesnych środowiskach IT.
4.	Aktualizacje i wsparcie zgodne z RODO	Produkt powinien zapewniać zgodność z RODO oraz umożliwiać bezpieczne zarządzanie danymi osobowymi.

5.1.3. Wsparcie, aktualizacje i rozwój

Lp.	Wymaganie	Wyjaśnienie
1.	Okresowa publikacja wersji z nowymi funkcjami	System powinien otrzymywać aktualizacje z nowymi funkcjami co najmniej raz na rok.
2.	Wsparcie dla wcześniejszych wersji produktu	Producent powinien zapewniać wsparcie techniczne dla starszych wersji produktu przez minimum 3 lata od ich publikacji.

3.	Baza danych wsparcia i zasoby online	Producent powinien oferować dostęp do portalu wsparcia technicznego oraz zasobów online, takich jak bazy wiedzy i fora.
4.	Transparentna polityka prywatności	Firma powinna udostępniać publicznie politykę prywatności, która wyjaśnia, w jaki sposób dane użytkowników są przechowywane i zabezpieczane.
5.	Zgodność z lokalnymi wymogami prawnymi	Produkt powinien być zgodny z lokalnymi wymogami prawnymi dotyczącymi przechowywania danych i zabezpieczeń.

5.2. Wymagania dla systemu Network Access Control

5.2.1. Podstawowe funkcjonalności oraz wymagania

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Aktywne zapobieganie dostępowi do sieci nieautoryzowanych użytkowników i urządzeń	System powinien wykrywać próby podłączenia do sieci i blokować nieautoryzowane urządzenia oraz użytkowników.	Mechanizmy kontroli dostępu do sieci oparte o 802.1X, Captive Portal, RADIUS oraz polityki bezpieczeństwa.
2	Wsparcie dla środowisk multi-vendor	System powinien współpracować z urządzeniami różnych producentów.	Integracja za pomocą standardowych protokołów (SNMP, RADIUS, syslog, API, CLI) niezależnych od producenta.
3	Zarządzanie przez interfejs WEB	Administratorzy powinni mieć dostęp do zarządzania systemem przez przeglądarkę.	Centralny panel zarządzania dostępny przez przeglądarkę w technologii HTML5 bez potrzeby instalacji wtyczek.
4	Instalacja rozproszona w ramach jednej licencji	Możliwość skalowania systemu przez instalację na wielu serwerach.	Obsługa architektury rozproszonej – instalacja wielu komponentów na osobnych serwerach fizycznych/wirtualnych w ramach jednej licencji.
5	Mechanizm Disaster Recovery	Umożliwienie odtworzenia działania systemu w przypadku awarii.	Automatyczna replikacja systemu i możliwość przełączenia do zapasowej instancji bez utraty danych.
6	Elastyczna rozbudowa licencyjna	System powinien wspierać wzrost liczby obsługiwanych urządzeń.	Możliwość dokupienia dodatkowych licencji bez konieczności zmiany architektury systemu.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Obsługa co najmniej 300 unikalnych autoryzacji dziennie z możliwością skalowania do 1000	System musi być skalowalny i wydajny.	Licencjonowanie oparte na liczbie autoryzacji z możliwością zwiększenia poprzez rozbudowę infrastruktury.
8	Zwolnienie licencji po rozłączeniu urządzenia	Optymalne wykorzystanie licencji poprzez ich rotację.	Licencja przypisywana dynamicznie podczas sesji i zwalniana po zakończeniu połączenia z siecią.
9	Obsługa agentów oraz BYOD	System musi wspierać autoryzację zarówno urządzeń zarządzanych, jak i prywatnych.	Możliwość jednoczesnej obsługi agentów oraz urządzeń BYOD zgodnie z licencjonowaną liczbą sesji.
10	Instalacja na maszynach fizycznych, VM oraz PaaS	System musi być kompatybilny z różnymi środowiskami wdrożeniowymi.	Obsługa platform wirtualnych i fizycznych: VMware ESXi, Hyper-V, Proxmox, KVM, XenServer oraz serwery fizyczne zgodne ze specyfikacją.
11	Wbudowane serwery wspierające infrastrukturę NAC	System powinien dostarczać wymagane komponenty serwerowe do działania sieciowego systemu kontroli dostępu.	Zintegrowane moduły: RADIUS, OTP, SYSLOG, TACACS+, monitoring, DHCP, polityki 802.1X oraz WWW dla Captive Portal.
12	Wysoka dostępność (High Availability)	Zapewnienie ciągłości działania w przypadku awarii komponentów systemu.	Redundancja dla kluczowych modułów (np. dostępu do sieci, DHCP) poprzez klastrowanie lub replikację.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
13	Uwierzytelnianie administratorów przez różne źródła	Możliwość autoryzacji administratorów przy użyciu wewnętrznych i zewnętrznych baz danych.	Obsługa m.in.: OpenLDAP, Active Directory, WebServices/API, Radius, MySQL, MSSQL, PostgreSQL, Oracle, ODBC.
14	Uwierzytelnianie tożsamości i urządzeń	Umożliwienie kontroli dostępu dla użytkowników i urządzeń na podstawie różnych źródeł autoryzacji.	Obsługa zewnętrznych systemów tożsamości, takich jak Active Directory, LDAP, Google Workspace, relacyjne bazy danych.
15	Synchronizacja danych z systemów zewnętrznych	Automatyczne pobieranie i aktualizacja danych z innych systemów zarządzania.	Integracja z systemami MDM, AD, bazami danych oraz systemami klasy ITSM (np. ServiceNow) i bezpieczeństwa (np. CheckPoint).
16	Mapowanie grup i tworzenie lokalnych danych uwierzytelniających	Dopasowanie struktury lokalnej systemu do danych z systemów zewnętrznych.	Możliwość przypisywania grup lokalnych do grup zdalnych, tworzenie certyfikatów i haseł oraz przysyłanie konfiguracji przez e-mail.
17	Wsparcie dla operacji masowych przez API	Możliwość automatyzacji zarządzania systemem.	API wspierające masowe operacje CRUD na obiektach systemu oraz funkcje blokowania dostępu.
18	Obsługa NTLM z wieloma serwerami AD	Możliwość autoryzacji w środowiskach z wieloma niezależnymi domenami AD.	Mechanizm autoryzacji NTLM bez wymogu relacji zaufania między domenami.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
19	Obsługa wielu PKI	Możliwość wykorzystania różnych źródeł certyfikatów dla różnych grup użytkowników.	System obsługuje wiele centrów certyfikacji w ramach różnych polityk i grup dostępu.
20	Tworzenie kont administracyjnych z konfigurowalnymi uprawnieniami	Precyzyjne definiowanie dostępu administratorów do funkcji systemu.	Możliwość przypisania uprawnień do konkretnych funkcji i obiektów zarządzanych w systemie.
21	Zmiana parametrów kont AD	Możliwość zarządzania kontami użytkowników Active Directory z poziomu systemu.	System umożliwia edycję parametrów kont (login, hasło, imię, nazwisko, e-mail, status) bezpośrednio z interfejsu administracyjnego.
22	Kontrola dostępu do elementów interfejsu i obiektów	Administratorzy powinni mieć różny poziom uprawnień do obiektów i funkcji.	Konfigurowalne prawa dostępu do menu systemowego oraz funkcji (dodawanie, edycja, usuwanie) zależnie od roli.
23	Wielojęzyczny interfejs graficzny	System musi być dostępny w co najmniej dwóch językach.	Interfejs użytkownika dostępny w języku polskim i angielskim, z możliwością rozszerzenia o inne wersje językowe.
24	Ograniczanie dostępu do interfejsu na podstawie adresu IP	Zabezpieczenie interfejsu administracyjnego przed nieautoryzowanym dostępem.	Możliwość definiowania list adresów IP lub podsieci, z których możliwy jest dostęp do panelu administracyjnego.
25	Raportowanie podłączonych tożsamości i urządzeń	Administratorzy powinni mieć wgląd w szczegółowe	Raporty zawierające dane o tożsamości, adresie MAC, urządzeniu, porcie, SSID,

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		dane o podłączonych użytkownikach.	urządzeniu sieciowym, VLAN, IP i statusie autoryzacji.
26	Centralne monitorowanie urządzeń sieciowych	Umożliwienie podglądu stanu i struktury urządzeń sieciowych w jednym miejscu.	Dedykowany interfejs graficzny prezentujący widok wszystkich portów i modułów zarządzanych urządzeń.
27	Monitoring urządzeń przez SNMP	System powinien wykorzystywać standardowe protokoły do zbierania danych.	Obsługa protokołu SNMP (co najmniej v1, v2c, v3) do monitoringu urządzeń końcowych i sieciowych.
28	Inwentaryzacja i sprawdzanie kondycji urządzeń	Zbieranie danych o sprzęcie oraz jego stanie.	System zbiera dane inwentaryzacyjne i stan urządzeń przy użyciu SNMP oraz analizuje zmiany i kondycję infrastruktury.
29	Zarządzanie konfiguracją portów i urządzeń sieciowych	Administrator powinien mieć możliwość zdalnej konfiguracji urządzeń.	System umożliwia zmianę ustawień VLAN, autoryzacji, opisu i statusu portów oraz zapis konfiguracji urządzeń.
30	Egzekwowanie polityk bezpieczeństwa w sieciach LAN i WLAN	System powinien wymuszać polityki bezpieczeństwa na urządzeniach sieciowych.	Mechanizm automatycznego wdrażania polityk dostępu i bezpieczeństwa na urządzeniach przewodowych i bezprzewodowych.
31	Konfiguracja serwera DHCP	System powinien zarządzać adresacją IP w wydzielonych podsieciach.	Możliwość tworzenia i konfiguracji własnych serwerów DHCP przypisanych do określonych podsieci IP.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
32	Własne szablony e-mail i wydruku poświadczeń	Możliwość dostosowania komunikacji z użytkownikiem do polityki firmy.	Konfigurowalne szablony wiadomości e-mail oraz wydruki zawierające dane dostępowe dla użytkowników.
33	Automatyczne wyszukiwanie urządzeń w podsieciach	System powinien skanować sieć i wykrywać nowe urządzenia.	Wbudowany skaner sieciowy działający co najmniej na podstawie SNMP v1, v2c, v3, umożliwiający automatyczne wykrywanie urządzeń.
34	Wysyłanie zdarzeń do systemów zewnętrznych	Integracja z systemami bezpieczeństwa i SIEM.	System umożliwia przesyłanie zdarzeń z serwerów autoryzacyjnych, DHCP, VPN, OTP i Tacacs+ przez Syslog.
35	Cykliczna kopia bezpieczeństwa	Zapewnienie ochrony danych poprzez regularne backupy.	Możliwość konfiguracji automatycznego tworzenia kopii zapasowej lokalnie lub na zasobach sieciowych.
36	Wbudowany Captive Portal	System powinien umożliwiać obsługę użytkowników końcowych przez portal logowania.	Wbudowany portal uwierzytelniania i rejestracji tożsamości/urządzeń (BYOD), dostępny bez konieczności integracji z zewnętrznymi rozwiązaniami.
37	Logowanie przez portale społecznościowe	Umożliwienie alternatywnych metod logowania dla użytkowników gościnnych.	Obsługa logowania przez Facebook, Google, LinkedIn w ramach Captive Portalu.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
38	Wysyłanie danych rejestracyjnych przez e-mail i SMS	System powinien umożliwiać wielokanałową dystrybucję danych dostępowych.	Wysyłanie danych przez e-mail, główną oraz zapasową bramkę SMS, z możliwością personalizacji treści.
39	Personalizacja strony gościnnej	Captive Portal powinien odpowiadać identyfikacji wizualnej organizacji.	Możliwość edycji wyglądu strony Captive Portal, m.in. logo, kolory, komunikaty, układ.
40	Responsywność Captive Portalu	Użytkownik powinien otrzymać stronę dopasowaną do urządzenia.	Portal dynamicznie dostosowuje wygląd do rodzaju urządzenia końcowego (komputer, tablet, telefon).
41	Rejestracja gości z potwierdzeniem sponsora	Goście powinni móc uzyskać dostęp do sieci po zatwierdzeniu przez uprawnionego użytkownika.	Captive Portal umożliwia tworzenie kont gości z mechanizmem potwierdzania przez sponsorów.
42	Dwuskładnikowe uwierzytelnianie (OTP)	Zwiększenie bezpieczeństwa dostępu do sieci przez dodatkową weryfikację.	Captive Portal obsługuje OTP przez Google Authenticator oraz SMS z wykorzystaniem podstawowej i zapasowej bramki SMS.
43	Logowanie przez konta lokalne i AD	System powinien wspierać różne metody uwierzytelniania.	Captive Portal umożliwia logowanie użytkowników lokalnych oraz domenowych (Active Directory).
44	Zmiana hasła przez Captive Portal	Użytkownicy powinni mieć możliwość samodzielnej zmiany hasła.	Możliwość zmiany hasła dla kont lokalnych oraz kont z Active

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
			Directory bezpośrednio w Captive Portalu.
45	Logowanie typu HotSpot	Umożliwienie szybkiego dostępu do sieci za pomocą kodu.	Captive Portal wspiera jednorazowe logowanie na podstawie kodu dostępu wygenerowanego przez administratora.
46	Dynamiczne pola formularza rejestracyjnego	Formularze powinny być dostosowane do potrzeb organizacji.	Tworzenie własnych pól formularza: tekst, lista rozwijana, checkboxy – konfigurowalne z poziomu interfejsu.
47	Wielojęzyczny interfejs Captive Portalu	Portal powinien być zrozumiały dla użytkowników różnych narodowości.	Interfejs Captive Portal dostępny co najmniej w językach: polski, angielski, niemiecki, hiszpański, francuski, ukraiński.
48	Pobieranie konfiguracji OTP	Użytkownicy powinni mieć możliwość łatwego skonfigurowania uwierzytelniania dwuskładnikowego.	Captive Portal udostępnia plik z konfiguracją OTP do zaimportowania do aplikacji (np. Google Authenticator).
49	Automatyczne kasowanie kont gościnnych	System powinien usuwać nieaktywne lub przeterminowane konta.	Obsługa cyklicznego usuwania kont gościnnych: ręcznie, po określonej liczbie dni lub przy wygaszeniu dostępu.
50	Konfiguracja limitu nieudanych logowań	Ochrona przed próbami nieautoryzowanego logowania.	Możliwość ustawienia maksymalnej liczby nieudanych prób logowania i powiązanych działań (np. blokada konta).

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
41	Rejestracja gości z potwierdzeniem sponsora	Goście powinni móc uzyskać dostęp do sieci po zatwierdzeniu przez uprawnionego użytkownika.	Captive Portal umożliwia tworzenie kont gości z mechanizmem potwierdzania przez sponsorów.
42	Dwuskładnikowe uwierzytelnianie (OTP)	Zwiększenie bezpieczeństwa dostępu do sieci przez dodatkową weryfikację.	Captive Portal obsługuje OTP przez Google Authenticator oraz SMS z wykorzystaniem podstawowej i zapasowej bramki SMS.
43	Logowanie przez konta lokalne i AD	System powinien wspierać różne metody uwierzytelniania.	Captive Portal umożliwia logowanie użytkowników lokalnych oraz domenowych (Active Directory).
44	Zmiana hasła przez Captive Portal	Użytkownicy powinni mieć możliwość samodzielnej zmiany hasła.	Możliwość zmiany hasła dla kont lokalnych oraz kont z Active Directory bezpośrednio w Captive Portalu.
45	Logowanie typu HotSpot	Umożliwienie szybkiego dostępu do sieci za pomocą kodu.	Captive Portal wspiera jednorazowe logowanie na podstawie kodu dostępu wygenerowanego przez administratora.
46	Dynamiczne pola formularza rejestracyjnego	Formularze powinny być dostosowane do potrzeb organizacji.	Tworzenie własnych pól formularza: tekst, lista rozwijana, checkboxy – konfigurowalne z poziomu interfejsu.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
47	Wielojęzyczny interfejs Captive Portalu	Portal powinien być zrozumiały dla użytkowników różnych narodowości.	Interfejs Captive Portal dostępny co najmniej w językach: polski, angielski, niemiecki, hiszpański, francuski, ukraiński.
48	Pobieranie konfiguracji OTP	Użytkownicy powinni mieć możliwość łatwego skonfigurowania uwierzytelniania dwuskładnikowego.	Captive Portal udostępnia plik z konfiguracją OTP do zaimportowania do aplikacji (np. Google Authenticator).
49	Automatyczne kasowanie kont gościnnych	System powinien usuwać nieaktywne lub przeterminowane konta.	Obsługa cyklicznego usuwania kont gościnnych: ręcznie, po określonej liczbie dni lub przy wygaszeniu dostępu.
50	Konfiguracja limitu nieudanych logowań	Ochrona przed próbami nieautoryzowanego logowania.	Możliwość ustawienia maksymalnej liczby nieudanych prób logowania i powiązanych działań (np. blokada konta).
61	Współpraca z serwerem tokenów	System powinien obsługiwać zewnętrzne źródła OTP.	Integracja z serwerem tokenów umożliwia uwierzytelnianie dwuskładnikowe np. przez OTP w VPN i Captive Portal.
62	Autokonfiguracja sieci dla urządzeń końcowych	System powinien automatycznie konfigurować ustawienia sieciowe urządzeń.	Mechanizm autokonfiguratora sieci dla Windows, macOS, iOS, Android umożliwia bezobsługowe połączenie z siecią firmową.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
63	Instalacja certyfikatu użytkownika końcowego przez autokonfigurator	Użytkownicy powinni otrzymać niezbędny certyfikat bez udziału administratora.	Autokonfigurator umożliwia automatyczne zainstalowanie certyfikatu użytkownika końcowego podczas konfiguracji sieci.
64	Wsparcie dla IPv6	System powinien być zgodny z nowoczesnymi protokołami sieciowymi.	Obsługa IPv6 dla komponentów: SSH, RADIUS, NTP, SNMP, komunikacji z Active Directory.

5.2.2. Mechanizmy uwierzytelniania

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Obsługa protokołów RADIUS oraz RADIUS Proxy	Możliwość komunikacji z serwerami autoryzacyjnymi w architekturze NAC.	System działa jako RADIUS oraz jako RADIUS Proxy przekazując zapytania do zewnętrznych serwerów.
2	Uwierzytelnianie przez MAC, PAP, CHAP, SNMP, 802.1X	Wsparcie różnych metod identyfikacji użytkowników i urządzeń.	System akceptuje uwierzytelnianie oparte o MAC, PAP/ASCII, CHAP, SNMP i 802.1X zgodnie z konfiguracją.
3	Wybór metody uwierzytelniania	Umożliwienie szczegółowego dostosowania protokołów uwierzytelniania.	Konfigurowalne opcje jak PEAP, EAP-TLS, EAP-TTLS, TEAP, MAC CHAP/MAC PAP itd.
4	Uwierzytelnianie 802.1X	Obsługa standardowego uwierzytelniania w sieciach przewodowych i bezprzewodowych.	Uwierzytelnienie urządzeń i użytkowników końcowych w oparciu o 802.1X z RADIUS.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
5	Uwierzytelnianie SNMP Trap	Obsługa komunikatów SNMP do celów autoryzacyjnych.	Reakcja na pułapki SNMP (Traps) wysyłane przez urządzenia końcowe jako forma autoryzacji.
6	Obsługa wielu suplikantów 802.1X	Zgodność z różnymi systemami operacyjnymi.	Kompatybilność z suplicantami z Windows (XP–11), macOS, iOS, Android, Ubuntu.
7	Tworzenie polityk uwierzytelniania opartych o złożone reguły	Możliwość warunkowania dostępu w oparciu o wiele parametrów.	Reguły oparte o tożsamość, grupy, OS, AD, urządzenia, porty, SSID, czas, metodę autoryzacji, Captive Portal.
8	Przypisywanie VLAN i atrybutów RADIUS VSA	Dynamiczne nadawanie polityk dostępu w trakcie autoryzacji.	Przesyłanie atrybutów takich jak VLAN, ACL, QoS do urządzeń sieciowych różnych producentów (Cisco, Aruba, itp.).
9	IP-to-ID Mapping	Powiązanie danych identyfikujących użytkownika i urządzenie.	Mapowanie adresu MAC, IP i ID użytkownika dla celów raportowania, polityk i inspekcji.
10	Funkcjonalność auto rejestracji	Automatyczne tworzenie powiązań tożsamości i urządzenia.	Identyfikacja i rejestracja urządzenia oraz przypisanie do użytkownika za pomocą SNMP, DHCP, NMAP, WMI.
11	Centralne wdrażanie polityk	Administrator powinien móc konfigurować dostęp z jednego miejsca.	Polityki bezpieczeństwa konfigurowane i egzekwowane z poziomu jednej konsoli systemu.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
12	Lokalna baza tożsamości	Możliwość autoryzacji użytkowników lokalnie bez zewnętrznego źródła.	Baza lokalna budowana ręcznie lub z pliku CSV.
13	Lokalna baza urządzeń końcowych	System powinien przechowywać dane urządzeń końcowych lokalnie.	Dodawanie urządzeń ręcznie lub z pliku CSV, z możliwością edycji.
14	Konfiguracja czasu ważności haseł gościnnych	Zwiększenie bezpieczeństwa przez ograniczenie czasu dostępu.	Możliwość ustawienia czasu ważności hasła w dniach przy tworzeniu kont gości.
15	Tworzenie hasła dnia	Ułatwienie logowania gości za pomocą jednego hasła.	Generowanie dziennego hasła przez Captive Portal dla gości.
16	Tworzenie lokalnej bazy urządzeń na podstawie MAC	Automatyczne budowanie bazy urządzeń na podstawie unikalnych identyfikatorów.	Tworzenie obiektów w lokalnej bazie na podstawie MAC – ręcznie lub z pliku CSV.
17	Uwierzytelnienie na podstawie adresów MAC	Dostęp do sieci powinien być możliwy na podstawie MAC.	Porównywanie adresów MAC z lokalną bazą urządzeń końcowych.
18	Obsługa różnych typów autoryzacji na jednym porcie	System powinien umożliwiać elastyczną konfigurację portów.	Obsługa autoryzacji pojedynczej, wielokrotnej, Voice VLAN, Captive Portal i innych równocześnie na jednym porcie.
19	Integracja z EDUROAM	System powinien wspierać federacyjną autoryzację użytkowników akademickich.	Wsparcie dla standardów i wymagań EDUROAM: 802.1X, RADIUS Proxy, federacja tożsamości.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
20	Przesyłanie danych do systemów zewnętrznych	Możliwość informowania innych systemów o wynikach autoryzacji.	Przesyłanie przez HTTP/REST danych takich jak ID użytkownika, MAC, IP do systemów zewnętrznych lub urządzeń.

5.2.3. Obsługa serwerów certyfikatów CA

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Zintegrowany serwer CA oraz współpraca z zewnętrznymi serwerami CA	System powinien umożliwiać własne zarządzanie certyfikatami oraz integrację z zewnętrzną infrastrukturą klucza publicznego.	Wbudowany serwer CA oraz możliwość integracji z zewnętrznymi CA poprzez standardowe protokoły, np. SCEP, OCSP.
2.1	Generowanie i podpisywanie certyfikatów dla tożsamości i urządzeń	Możliwość wystawiania certyfikatów nie tylko dla użytkowników, ale również urządzeń końcowych.	Funkcja CA systemu umożliwia tworzenie certyfikatów X.509 dla użytkowników i urządzeń z użyciem własnego lub zewnętrznego CA.
2.2	Bezpieczne przechowywanie certyfikatów	System musi chronić certyfikaty przed nieautoryzowanym dostępem.	Certyfikaty przechowywane są w zaszyfrowanej bazie lub kontenerze certyfikatów zabezpieczonym hasłem/kluczem.
2.3	Generowanie certyfikatów przez SCEP	Wsparcie dla automatycznego wystawiania certyfikatów w systemach końcowych.	Protokół SCEP obsługiwany przez CA pozwala urządzeniom na żądanie certyfikatu w sposób zautomatyzowany.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
2.4	Obsługa OCSP	System powinien umożliwiać sprawdzanie ważności certyfikatów online.	Zintegrowany lub zewnętrzny serwer OCSP umożliwia walidację statusu certyfikatu bez konieczności pobierania CRL.

5.2.4. Obsługa serwerów DHCP

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Zintegrowany serwer DHCP	System powinien mieć własny mechanizm przydzielania adresów IP.	Wbudowany moduł serwera DHCP działający bez potrzeby integracji z zewnętrznym serwerem.
2	Auto rejestracja urządzenia przez serwer DHCP	Możliwość automatycznego tworzenia powiązań urządzeń i adresów MAC w momencie nadania IP.	DHCP rejestruje urządzenie w systemie na podstawie adresu MAC przy pierwszym przydzieleniu IP.
3.1	Uruchamianie DHCP dla wybranych podsieci	Możliwość skonfigurowania usług DHCP tylko tam, gdzie to konieczne.	Administrator definiuje, które podsieci obsługiwane są przez serwer DHCP.
3.2	Przypisanie stałego IP dla MAC	Rezerwacja adresu IP dla konkretnego urządzenia.	Możliwość przypisania statycznego adresu IP dla danego adresu MAC w konfiguracji DHCP.
3.3	Różne IP dla MAC w różnych podsięciach	Taki sam adres MAC może mieć różne IP zależnie od lokalizacji w sieci.	Konfiguracja rezerwacji IP zależnie od przypisania MAC do konkretnej podsieci.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
3.4	Ograniczenie dzierżawy tylko dla wybranych MAC	Zwiększenie bezpieczeństwa przez filtrowanie urządzeń.	DHCP udostępnia adresy tylko urządzeniom z listy dozwolonych adresów MAC.
3.5	Blokada wybranych MAC	Zapobieganie dostępowi dla nieautoryzowanych urządzeń.	Możliwość blokowania przydziału adresów IP dla określonych adresów MAC.
3.6	Monitoring DHCP – obciążenie, błędy, ograniczenia	Administratorzy muszą mieć wgląd w działanie i problemy DHCP.	System monitoruje m.in. liczbę przydzielonych adresów, błędów decline, braków konfiguracji, ograniczenia dla MAC.
3.7	Ustawienia parametrów DHCP	Możliwość konfigurowania dodatkowych opcji przekazywanych klientom.	Obsługa dodatkowych opcji DHCP (np. DNS, router domyślny, domena lokalna).
3.8	Graficzny podgląd wykorzystania adresów IP	Ułatwienie zarządzania i planowania adresacji.	Widok podsieci z graficznym podziałem adresów IP na przydzielone statycznie i dynamicznie.
3.9	Dynamiczny → statyczny przydział bez restartu	Przekształcanie dynamicznego IP w statyczne bez przerwy w pracy.	Możliwość przekształcenia przypisanego dynamicznie IP w rezerwację statyczną bez restartu usługi DHCP.
3.10	Zmiany bez przerywania działania serwera	Wysoka dostępność konfiguracji DHCP.	Modyfikacje ustawień DHCP możliwe są bez przerywania pracy serwera DHCP.

5.2.5. Obsługa serwerów TACACS+

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Grupowanie urządzeń końcowych i administratorów	Umożliwienie zarządzania uprawnieniami w sposób zorganizowany i skalowalny.	Administrator może tworzyć grupy urządzeń oraz grupy administratorów do stosowania polityk uprawnień.
2	Tworzenie haseł dla administratorów	System powinien pozwalać na centralne zarządzanie poświadczeniami administracyjnymi.	Możliwość tworzenia i zarządzania hasłami administratorów z poziomu interfejsu systemu.
3	Lista komend uprawnień dla administratorów	Definiowanie, jakie komendy są dozwolone dla konkretnego administratora lub grupy.	Tworzenie i przypisywanie list komend (Command Sets) do ról lub użytkowników, np. dla TACACS+.
4	Raportowanie wszystkich wydanych komend	Pełna audytowalność działań administratorów na urządzeniach sieciowych.	System rejestruje każdą komendę wykonaną przez administratora na zarządzanym urządzeniu (np. przez TACACS+).
5	Zmiana hasła administratora z poziomu urządzenia wg harmonogramu	Automatyzacja polityki bezpieczeństwa haseł.	System umożliwia zdalną, cykliczną zmianę hasła administratora na urządzeniu sieciowym zgodnie z ustalonym interwałem czasowym.
6	Logowanie przez Microsoft Active Directory	Wsparcie integracji z domeną organizacyjną dla administracji.	Autoryzacja administratorów przez konta domenowe AD, z wykorzystaniem LDAP/LDAPS lub RADIUS.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Logowanie przez tokeny OTP	Zwiększenie bezpieczeństwa poprzez uwierzytelnianie dwuskładnikowe.	Logowanie administratorów wspierane przez jednorazowe hasła generowane przez np. Google Authenticator, SMS.
8	Przypisywanie atrybutów zwrotnych VSA podczas autoryzacji	Wysyłanie do urządzeń danych definiujących poziom dostępu i uprawnienia.	W ramach RADIUS/TACACS+ system przesyła VSA (Vendor-Specific Attributes), definiujące np. poziom dostępu do urządzenia.

5.2.6. Raportowanie i monitoring

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Monitoring autoryzacji	Bieżący podgląd oraz historia autoryzacji do sieci.	System prezentuje dane o udanych i nieudanych autoryzacjach w czasie rzeczywistym oraz w raportach.
2	Monitoring zdarzeń systemowych	Śledzenie działania komponentów systemu i wykrywanie błędów.	Logi zdarzeń i statusów systemowych dostępne w interfejsie WWW, CLI i eksportowane w raportach.
3	Monitoring zdarzeń DHCP	Kontrola pracy serwera DHCP oraz analiza nadanych adresów.	Rejestracja, wizualizacja i raportowanie logów DHCP, w tym błędów i przypisań.
4	Monitoring tożsamości	Podgląd aktywności i historii logowania tożsamości.	System wyświetla listę zalogowanych użytkowników, ostatnie logowania, powiązane urządzenia i sesje.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
5	Monitoring urządzeń końcowych	Bieżący stan i dane urządzeń końcowych.	Monitoring m.in. systemu operacyjnego, wersji, ostatniej autoryzacji, przypisanych polityk, adresów IP/MAC.
6	Monitoring urządzeń sieciowych	Podgląd statusu urządzeń infrastruktury sieciowej.	Wizualizacja stanu portów, wydajności, dostępności, alarmów urządzeń sieciowych przewodowych i bezprzewodowych.
7	Raport stanu systemu z pełnymi szczegółami	Szczegółowy raport o stanie infrastruktury systemu NAC.	Dostępny przez CLI, WWW i e-mail. Zawiera m.in. dane z nodów, wykorzystanie polityk, błędy, statusy, obciążenia, konfiguracje, porty.
8	Raport logowań z IP	Raportowanie sesji logowania użytkownika z przypisanym adresem IP.	System zestawia dane tożsamości z nadanym IP oraz informacją o czasie logowania.
9	Raport stanu systemu z poziomu CLI	Szybki dostęp do podstawowych informacji diagnostycznych.	Dostępne z CLI dane: CPU, RAM, przestrzeń dyskowa, stan usług.
10	Logi DHCP z informacją o polityce dostępu	Powiązanie przypisań IP z zastosowaną polityką bezpieczeństwa.	Logi DHCP zawierają informacje o tym, jaką politykę przypisano do danego urządzenia przy autoryzacji.
11	Graficzny podgląd stanu przełączników i portów	Intuicyjny podgląd kondycji portów i przełączników w czasie rzeczywistym.	Interfejs graficzny z wizualizacją zajętości, stanu portów (down/up), nazw i VLANów.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
12	Graficzny podgląd urządzeń w stosie	Wsparcie dla topologii urządzeń sieciowych działających jako stos.	Interfejs prezentuje strukturę stosów (stack) oraz status każdego urządzenia i portu w tej architekturze.
13	Graficzna wizualizacja niezgodności VLAN	Wykrywanie błędów konfiguracji VLAN w środowisku sieciowym.	System wykrywa niespójności przypisać VLANów i prezentuje je wizualnie w panelu administratora.
14	Monitoring zasobów drukarek sieciowych	Śledzenie stanu i materiałów eksploatacyjnych drukarek.	System gromadzi dane o zasobach drukarek (toner, stan, błędy) i prezentuje je graficznie.
15	Graficzny podgląd stanu tożsamości i urządzeń	Monitorowanie aktywności użytkowników i ich urządzeń końcowych.	Interfejs graficzny prezentuje dane takie jak system, ostatnia autoryzacja, aktywność na dzień, historia użycia.
16	Bieżący podgląd zalogowanych tożsamości i urządzeń	Widoczność użytkowników zalogowanych przez różne kontrolery i urządzenia.	Widok w czasie rzeczywistym z podziałem na urządzenia sieciowe i kontrolery WiFi, z listą zalogowanych tożsamości.
17	Raport z logów OTP	Śledzenie poprawnych i błędnych autoryzacji z użyciem OTP.	System raportuje skuteczne/błędne próby OTP, wysłane tokeny przez SMS i statusy.
18	Raport zdarzeń Microsoft Active Directory	Rejestracja operacji logowania związanych z domeną.	Rejestracja logowań/wylogowań oraz błędnych logowań do systemu i do sieci 802.1X przez AD.

5.2.7. Alarmy

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Generowanie alarmów systemowych przez e-mail, Syslog i notyfikacje	System powinien automatycznie powiadamiać administratorów o sytuacjach krytycznych.	System wysyła alarmy przez e-mail, Syslog i wewnętrzne powiadomienia w GUI w przypadku wykrycia krytycznego zdarzenia.
2.1	Alarmy dla wysokiej liczby transakcji RADIUS	Wykrywanie przeciążenia systemu na poziomie autoryzacji.	System analizuje liczbę transakcji RADIUS i generuje alerty, gdy przekroczone są zdefiniowane progi.
2.2	Alarmy dla opóźnień w obsłudze RADIUS	Monitorowanie wydajności autoryzacji.	Alerty są generowane w przypadku przekroczenia zadanego czasu odpowiedzi na zapytania RADIUS.
2.3	Alarmy dla krytycznego statusu modułów	System powinien zgłaszać awarie komponentów.	Alerty w sytuacji błędu działania lub braku dostępności krytycznych usług systemu.
3	Narzędzia diagnostyczne w systemie	Administrator powinien mieć dostęp do narzędzi rozwiązywania problemów z poziomu interfejsu.	System udostępnia zestaw narzędzi do analizy łączności, ruchu sieciowego i błędów autoryzacji.
3.1	Test łączności IP – ping i traceroute	Podstawowa weryfikacja połączeń między komponentami.	Narzędzia ping i traceroute dostępne z poziomu GUI i CLI do sprawdzania dostępności hostów.
3.2	Analiza ruchu – tcpdump dla RADIUS i TACACS+	Diagnozowanie ruchu autoryzacyjnego.	Możliwość filtrowania i przechwytywania pakietów

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
			protokołów RADIUS i TACACS+ w czasie rzeczywistym.
3.3	Wyszukiwanie zdarzeń RADIUS po parametrach	Weryfikacja logów autoryzacji z dokładnym filtrowaniem.	Wyszukiwanie zdarzeń wg użytkownika, MAC, statusu (sukces/porażka), przyczyny błędu oraz daty i godziny.
3.4	Wykonywanie zdalnych poleceń na urządzeniach sieciowych	Umożliwienie bezpośredniego reagowania na problemy w infrastrukturze.	System umożliwia wykonanie zdalnych komend (np. CLI) na urządzeniach w celu szybkiej diagnostyki i korekty konfiguracji.

5.2.8. Wymagania dotyczące wdrożenia i harmonogram ramowy

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Dostawa, instalacja i zalicencjonowanie systemu	System musi zostać w pełni wdrożony w środowisku klienta.	Instalacja fizyczna/wirtualna, aktywacja licencji oraz przygotowanie środowiska do dalszej konfiguracji.
2	Wstępna konfiguracja systemu NAC	Konieczne jest uruchomienie kluczowych elementów systemu.	Integracja z AD, konfiguracja urzędu certyfikacji (CA), włączenie funkcji wysokiej dostępności (HA).
3	Konfiguracja firewalla – VLAN gościnny i polityki	System powinien obsługiwać ruch sieciowy zgodnie z politykami bezpieczeństwa.	Dodanie VLAN dla gości, konfiguracja reguł dostępu, NAT itp. na wskazanym urządzeniu UTM/firewall.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
4	Import tożsamości i urządzeń końcowych	System musi być zasilony danymi użytkowników i urządzeń.	Import danych z Active Directory oraz z plików (list) dostarczonych przez Zamawiającego.
5	Integracja z urządzeniami sieciowymi	System NAC powinien współpracować z istniejącą infrastrukturą.	Integracja przełączników, access pointów itd. z systemem NAC zgodnie z obsługiwanymi funkcjami (np. SNMP, 802.1X).
6	Testowe uruchomienie autoryzacji 802.1X EAP-TLS	Należy wykazać poprawność konfiguracji uwierzytelniania certyfikatowego.	Konfiguracja przykładowych urządzeń końcowych z każdej serii i przeprowadzenie testów autoryzacji 802.1X (EAP-TLS).
7	Testowe uruchomienie autoryzacji na podstawie MAC	Należy wykazać poprawność alternatywnego mechanizmu autoryzacji.	Konfiguracja autoryzacji MAC z korelacją do DHCP, SNMP i port scanningiem, przeprowadzenie testów.
8	Szkolenie administratorów	Administratorzy muszą zostać przeszkoleni z obsługi systemu.	Dwudniowe szkolenie online (zdalne), do 4 osób, po 5 godzin dziennie – zakres: konfiguracja, administracja, diagnostyka.
9	Dokumentacja powykonawcza	Po wdrożeniu musi powstać dokumentacja techniczna z opisem konfiguracji.	Opracowanie i przekazanie Zamawiającemu dokumentu zawierającego opis wykonanych prac, konfiguracji i urządzeń – w ciągu 14 dni od zakończenia wdrożenia.

5.2.9. Licencja i wsparcie techniczne producenta oprogramowania

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Dożywotnia licencja systemu NAC z min. 12-miesięcznym wsparciem producenta	Licencja na system ma być bezterminowa, a wsparcie techniczne musi być aktywne przez co najmniej rok.	Wykonawca dostarcza licencję bez ograniczenia czasowego oraz min. roczne wsparcie techniczne producenta zgodne z ofertą.
2	Kontakt mailowy z działem wsparcia technicznego	Możliwość zgłaszania problemów i zapytań dotyczących systemu bezpośrednio do producenta.	Producent systemu udostępnia kanał e-mail do obsługi zgłoszeń technicznych.
3	Rozwiązywanie powtarzalnych problemów i wsparcie w analizie problemów trudnych do powtórzenia	Użytkownik ma otrzymać pomoc zarówno w typowych przypadkach, jak i przy incydentach trudnych do jednoznacznego odtworzenia.	Producent analizuje zgłoszenia, zapewnia poprawki oraz wsparcie diagnostyczne dla problemów nieoczywistych.
4	Wsparcie w konfiguracji i obejściach problemów	Pomoc w dostrojeniu systemu oraz dostarczanie tymczasowych rozwiązań do czasu naprawy.	Zespół wsparcia pomaga ustalić właściwe parametry konfiguracyjne oraz zaleca rozwiązania tymczasowe dla błędów.
5	Dostęp do dokumentacji i instrukcji online	Użytkownik powinien mieć dostęp do aktualnych materiałów pomocniczych.	Producent udostępnia dokumentację, poradniki i instrukcje na swojej stronie internetowej lub w dedykowanym portalu wsparcia.
6	Dostęp do aktualizacji i poprawek z poziomu interfejsu	System powinien umożliwiać aktualizację bezpośrednio przez GUI.	Użytkownik może pobrać i zastosować aktualizacje oraz poprawki systemu

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
			bezpośrednio z interfejsu graficznego.

5.2.10. Szkolenia

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Przeprowadzenie warsztatów (1x5h) z obsługi systemu NAC	Użytkownicy końcowi muszą zdobyć wiedzę o wdrożonym systemie.	Zdalne warsztaty online prowadzone przez Wykonawcę
2	Zakres warsztatów dopasowany do wdrożonego systemu NAC	Szkolenie musi obejmować realnie wdrożone funkcje i konfigurację.	Program warsztatów obejmuje funkcje i konfigurację systemu wdrożonego u Zamawiającego.
3	Zaświadczenia uczestnictwa	Potwierdzenie udziału oraz zdobytej wiedzy.	Każdy uczestnik otrzymuje imienne zaświadczenie po zakończeniu warsztatów.
4	Forma zdalna	Szkolenie nie wymaga obecności fizycznej uczestników.	Warsztaty prowadzone online przy użyciu komunikatora uzgodnionego z Zamawiającym.
5	Materiały szkoleniowe w języku polskim	Uczestnicy powinni mieć dostęp do materiałów edukacyjnych.	Wykonawca dostarcza elektroniczne materiały szkoleniowe w języku polskim (PDF, prezentacje).
6	Uzgodnienie szczegółowego planu i	Terminy i zakres powinny odpowiadać potrzebom	Wykonawca uzgadnia harmonogram i agendę

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
	terminów z Zamawiającym	organizacyjnym Zamawiającego.	warsztatów z przedstawicielem Zamawiającego przed realizacją.

5.3. Wymagania dla systemu Privilege Access Management

5.3.1. Monitorowanie Aktywności Użytkowników

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Monitorowanie aktywności użytkowników w sesjach lokalnych i zdalnych	System powinien śledzić działania użytkowników niezależnie od typu sesji	Agent monitorujący działa zarówno lokalnie, jak i przy połączeniach zdalnych (np. RDP, SSH).
2	Rejestrowanie użytkowników korzystających z wielu monitorów	System powinien rejestrować aktywność na każdym z ekranów	Obsługa wielu ekranów przez agenta i zapis każdego strumienia wideo niezależnie.
3	Rejestrowanie jedynie aktywnego okna	Rejestrowana powinna być tylko aktywna aplikacja, z którą użytkownik faktycznie pracuje	Agent rozpoznaje i loguje tylko aktywne okno z wykluczeniem procesów działających w tle.
4	Monitorowanie schowka systemowego	System powinien rejestrować operacje kopiuj/wklej	Agent monitoruje zawartość schowka i zapisuje historię operacji.
5	Rejestrowanie naciśnięć klawiszy z możliwością późniejszego wyszukiwania	System powinien logować klawisze i umożliwiać ich analizę	Keystroke logging z możliwością filtrowania po czasie, aplikacji i sesji.
6	Nagrywanie audio	Rejestrowanie dźwięku może być wymagane w przypadku podejrzenia nadużyć	System umożliwia aktywację rejestracji audio w określonych sytuacjach (zgodnie z polityką).

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Monitorowanie przesyłanych plików	System powinien śledzić transfer plików np. przez e-mail, FTP, przeglądarkę	Agent wykrywa operacje kopiowania/wysyłania plików i zapisuje metadane.
8	Monitorowanie użycia USB	Rejestrowanie połączeń i użycia nośników USB	Wykrywanie urządzeń, logowanie czasu podłączenia/rozłączenia, ID urządzenia.
9	Monitorowanie odwiedzanych stron internetowych	System powinien śledzić aktywność przeglądarki	Agent monitoruje adresy URL, tytuły stron i czasy odwiedzin.
10	Monitorowanie zdalnych adresów IP i filtrowanie sesji	Identyfikacja źródeł zdalnych połączeń	Możliwość filtrowania sesji po IP źródłowym oraz geolokalizacja.
11	Podgląd sesji użytkownika na żywo	Administrator może nadzorować działania użytkownika w czasie rzeczywistym	Podgląd sesji z transmisją ekranu na żywo przez konsolę administracyjną.
12	Rejestrowanie aktywności użytkowników w systemie Linux	System powinien działać także w środowisku Linux	Agent Linux monitoruje aktywność terminala, procesy, sesje graficzne.
13	Rejestrowanie aktywności na podstawie alertów	Monitoring może być aktywowany przez zdefiniowane zdarzenia	System rejestruje tylko wtedy, gdy wystąpi określony warunek np. użycie USB.
14	Anonimizacja danych użytkowników	Ochrona prywatności monitorowanych danych	Możliwość ukrycia nazw kont, adresów e-mail i danych wrażliwych w raportach.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
15	Eksport wyników do formatu wideo	Sesje użytkownika mogą być archiwizowane jako wideo	System umożliwia eksport sesji w formacie MP4 do analizy lub archiwizacji.
16	Szyfrowanie wrażliwych danych	Dane powinny być chronione przed nieautoryzowanym dostępem	Szyfrowanie danych na poziomie agenta oraz po stronie serwera (np. AES-256).
17	Możliwość wyłączenia logowania klawiszy w wybranych aplikacjach	Zgodność z regulacjami prawnymi (np. bankowość, medycyna)	Lista wyjątków definiowana przez administratora – np. Word, przeglądarki.
18	Powiadomienie użytkownika o nagrywaniu sesji	Użytkownik powinien być świadomy monitoringu (jeśli wymagane)	Komunikat systemowy lub banner informujący o rejestracji sesji.
19	Wieloparametrowe wyszukiwanie w danych	Możliwość dokładnej analizy wyników	Filtrowanie po użytkowniku, czasie, aplikacji, adresie IP, rodzaju aktywności.
20	Rejestrowanie działań w systemie zarządzania	Monitoring zmian konfiguracji i działań administratorów	Agent rejestruje akcje w interfejsie zarządzającym systemem PAM.
21	Rejestrowanie danych wejściowych systemu Linux	Śledzenie poleceń wpisywanych w CLI	Logowanie interakcji z terminalem i środowiskiem tekstowym.
22	Archiwizacja sesji użytkownika	Sesje powinny być przechowywane do celów audytowych	Zapis sesji w archiwum z możliwością eksportu i odtworzenia.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
23	Przeglądanie zarchiwizowanych sesji	Dostęp do przeszłych sesji użytkownika	System umożliwia przeglądanie zarchiwizowanych sesji w formacie wideo.
24	Eksport pojedynczych zrzutów ekranu	Dla potrzeb raportowych	Możliwość wyeksportowania konkretnego momentu z sesji.
25	Walidacja eksportu	Zapewnienie integralności danych	System stosuje sumy kontrolne lub podpis cyfrowy dla plików eksportu.
26	Walidacja danych monitoringu	Zapewnienie, że dane monitorowane nie zostały zmienione	Mechanizmy integralności danych (hashowanie, podpisywanie).
27	Filtrowanie użytkowników	Możliwość analizy danych po użytkowniku	Filtrowanie wyników po loginie, grupie, adresie IP, czasie.
28	Filtrowanie aplikacji i stron	Ograniczenie danych do wybranych źródeł	System umożliwia selekcję tylko określonych aplikacji lub stron.
29	Monitoring tylko w godzinach pracy	Ograniczenie rejestracji do ustalonego harmonogramu	Możliwość ustawienia harmonogramu aktywności agenta.
30	Wykrywanie nietypowego logowania	System powinien wykrywać anomalie użytkownika	Identyfikacja rzadko używanych kont, komputerów, lokalizacji.
31	Wykrywanie użycia poza godzinami pracy	Wsparcie dla polityk bezpieczeństwa i zgodności	Alerty i raporty dla działań poza ustalonymi godzinami.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
32	Wykrywanie beczynności użytkownika	Pomiar produktywności i anomalii w pracy	Agent śledzi aktywność klawiatury, myszki i porównuje do czasu sesji.
33	Archiwizacja/usuwanie danych z zachowaniem metadanych	Zarządzanie retencją danych	Możliwość usuwania nagrań przy pozostawieniu logów metadanych.
34	Powiadomienie e-mail przy braku aktywności urzędnika	Alerty o utracie łączności z agentem	System wysyła powiadomienie, gdy agent przestaje raportować przez X minut.

5.3.2. Licencjonowanie

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Pływające licencje na punkty końcowe	Licencje powinny być dynamicznie przydzielane tylko aktywnym urządzeniom	System licencjonuje urządzenia końcowe na podstawie aktywności – po rozłączeniu licencja jest zwalniana i może być użyta przez inne urządzenie.
2	Oddzielne licencjonowanie dla aplikacji i funkcji	Umożliwienie elastycznej rozbudowy systemu według potrzeb organizacji	System oferuje modułowe licencje np. osobno na monitoring, sesje RDP, zarządzanie hasłami, co pozwala kupować tylko potrzebne funkcje.
3	Licencjonowanie oparte na użytkownikach	Alternatywny model dla środowisk z dużą rotacją urządzeń	System może być licencjonowany w oparciu o konkretne konta użytkowników zamiast urządzeń końcowych, np. dla pracy zdalnej lub sesji terminalowych.

5.3.3. Obsługiwane platformy

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Monitorowanie stacji roboczych i serwerów Windows, Mac, Linux, SELinux oraz Citrix	System powinien działać na szerokim wachlarzu systemów operacyjnych i środowisk serwerowych	Dedykowane agenty wspierają monitoring aktywności użytkowników na platformach Windows, macOS, dystrybucjach Linux, SELinux oraz w środowiskach Citrix.
2	Monitorowanie Amazon WorkSpaces	Wsparcie dla wirtualnych pulpitów chmurowych	Agent działa na instancjach WorkSpaces, zapewniając monitoring sesji użytkownika w środowisku zarządzanym przez AWS.
3	Wsparcie dla środowisk VDI z nieprzechowywalnym monitoringiem i płynającymi licencjami	Obsługa dynamicznych sesji desktopów wirtualnych	System wspiera monitoring VDI z dynamicznym przypisywaniem agentów i licencji do aktualnie zalogowanego użytkownika bez trwałego śledzenia urządzenia.
4	Monitorowanie systemu X Window	Wsparcie dla graficznych środowisk Linuksa opartych o X11	Agent rejestruje aktywność użytkownika w sesjach X11 (X Window System), w tym kliknięcia, aplikacje, terminal.
5	Monitorowanie i filtrowanie stron na macOS	System powinien działać również na komputerach Apple z możliwością filtrowania WWW	Agent macOS umożliwia rejestrację aktywności użytkownika oraz monitorowanie i filtrowanie odwiedzanych stron internetowych.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
6	Monitorowanie Ubuntu 22.04 z pulpitem Wayland	Wsparcie dla nowoczesnych środowisk graficznych Linuksa	Agent obsługuje sesje Wayland w Ubuntu 22.04, umożliwiając rejestrowanie aktywności użytkowników.
7	Wsparcie przekierowania X Window	Wsparcie dla środowisk z tunelowaniem X11	System umożliwia monitorowanie sesji użytkownika również w przypadku pracy zdalnej z użyciem przekierowania X Window.
8	Monitorowanie systemu AIX	Wsparcie dla systemów klasy UNIX stosowanych w środowiskach korporacyjnych	Agent tekstowy rejestruje aktywność użytkowników w sesjach terminalowych systemu AIX.
9	Rejestracja AppStream oraz Azure VDI/App	Wsparcie dla nowoczesnych środowisk wirtualizacji aplikacji	Agenci monitorują aktywność użytkowników korzystających z AppStream (AWS) oraz Azure Virtual Desktop i Azure App Service.

5.3.4. Wdrożenie

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Wersja lokalna (on-premise)	System musi być możliwy do zainstalowania w infrastrukturze klienta	Oprogramowanie dostępne w wersji on-premise jako samodzielne wdrożenie zarządzane przez klienta

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
2	Wersja SaaS	Możliwość wdrożenia w modelu chmurowym	Dostępna wersja hostowana przez producenta lub integratora, z dostępem przez Internet
3	Główny panel do monitorowania wielu odizolowanych wdrożeń	Konsola centralna do nadzoru rozproszonych instancji	Interfejs typu Management Console agregujący dane z wielu wdrożeń w jednym panelu
4	Tryb wielodzierżawny (multi-tenancy)	Możliwość izolowania danych i konfiguracji wielu organizacji w jednym wdrożeniu	System wspiera niezależnych tenantów z odseparowaną polityką i zasobami
5	Interfejs webowy do zarządzania	Zarządzanie całym systemem przez przeglądarkę internetową	WebGUI dostępny przez HTTPS, bez potrzeby instalacji dodatkowego oprogramowania
6	Instalacja klientów przez interfejs webowy	Szybka dystrybucja agentów z poziomu przeglądarki	Interfejs umożliwia generowanie i dystrybucję instalatorów z przypisanymi kluczami i politykami
7	Wysoka dostępność i odzyskiwanie po awarii z load balancingiem	Minimalizacja przestojów i zwiększenie odporności systemu	System wspiera redundancję głównych komponentów z integracją z load balancerami
8	Redukcja użycia pasma	Optymalizacja przesyłu danych między klientem a serwerem	Kompresja oraz ograniczanie rozdzielczości/ilości zrzutów ekranu w zależności od przepustowości

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
9	Monitorowanie problemów serwera centralnego i bazy danych	Wczesne ostrzeganie o awariach lub przeciążeniu	Wbudowany mechanizm kontroli stanu usług i przestrzeni z alertami mailowymi
10	Automatyczna aktualizacja komponentów	Zmniejszenie nakładu administracyjnego	System wspiera cykliczne aktualizacje agentów i komponentów serwera
11	Wsparcie dla Azure SQL	Elastyczność integracji z usługami chmurowymi	Możliwość podłączenia systemu do bazy danych w modelu Azure SQL
12	Szyfrowane połączenie z bazą danych	Ochrona przesyłanych danych	Komunikacja z bazą danych odbywa się przez szyfrowane kanały (np. TLS)
13	Wsparcie dla SQL Database jako storage	Elastyczność doboru backendu bazodanowego	Dane systemowe mogą być przechowywane w dowolnej relacyjnej bazie SQL
14	Przechowywanie danych w pamięciach obiektowych	Skalowalne archiwum danych	Możliwość użycia storage typu object (np. S3) do przechowywania nagrań, logów itp.
15	Przechowywanie plików	Wsparcie dla lokalnego lub sieciowego zapisu danych	System umożliwia zapisywanie plików na SMB, NFS, dyskach lokalnych
16	Wielohierarchiczne grupy kluczy prywatnych	Lepsze zarządzanie certyfikatami i bezpieczeństwem	Rozwiązanie umożliwia definiowanie struktury zarządzania kluczami w zależności od organizacji

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
17	API	Integracja z zewnętrznymi systemami	Publiczne API REST pozwala m.in. na pobieranie danych, sterowanie sesjami
18	Przeglądanie sesji przez API	Automatyzacja analizy sesji przez systemy SIEM/ITSM	API umożliwia dostęp do nagrań i metadanych sesji w celu zewnętrznej analizy

5.3.5. Zarządzanie dostępem i alertami

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Kontrola urządzeń USB z możliwością blokowania klas	Możliwość blokowania np. pamięci masowych lub urządzeń HID	System pozwala na definiowanie klas urządzeń USB i ich selektywną blokadę na monitorowanych punktach końcowych
2	Wsparcie dostępu wielu użytkowników z indywidualnymi uprawnieniami	Możliwość przydzielania ról użytkownikom systemu PAM	Mechanizm RBAC (Role-Based Access Control) pozwala na definiowanie dostępu do funkcji i danych
3	Automatyczna blokada USB przy naruszeniu bezpieczeństwa	USB mogą być wyłączone np. po wykryciu anomalii	System wspiera reakcję na incydenty – blokuje porty USB w odpowiedzi na wyzwalacze lub reguły
4	Wykrywanie parametrów naciśnięć klawiszy	Detekcja nietypowych wzorców zachowania użytkownika	System analizuje częstotliwość, czas i schemat pisania na

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
			klawiaturze jako warstwę analizy zachowań
5	Ochrona na poziomie jądra przed modyfikacją lub usunięciem plików sesji	Zapobieganie sabotażowi monitoringu	Monitor działa jako usługa z poziomu kernel-mode, zabezpieczona przed usunięciem przez administratorów lokalnych
6	Reguły alertów oparte o wyrażenia regularne	Możliwość tworzenia zaawansowanych reguł detekcji	Administratorzy mogą ustawić alerty np. na konkretne frazy, aplikacje, adresy URL
7	Uwierzytelnianie dwuskładnikowe (TOTP) dla użytkowników monitorowanych stacji	Dodatkowe zabezpieczenie dostępu do końcówek	Integracja z aplikacjami typu Google Authenticator zapewnia TOTP na poziomie logowania do systemu
8	Dodatkowe poświadczenia przy logowaniu	Możliwość zastosowania niestandardowych mechanizmów MFA	System wspiera weryfikację użytkownika na poziomie agenta przed uruchomieniem sesji
9	Blokowanie użytkowników po wykryciu zabronionych działań	Automatyczna reakcja na incydenty	System automatycznie zawiesza sesję lub konto po wykryciu działań niezgodnych z polityką
10	Zamykanie zabronionych aplikacji	Egzekwowanie polityki bezpieczeństwa	Możliwość ustawienia listy aplikacji zakazanych i ich automatyczne zamykanie przez agenta
11	Czarna lista użytkowników	Ograniczanie dostępu do systemu	Lista zakazanych użytkowników lub adresów może być konfigurowana ręcznie lub automatycznie

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
12	Wymaganie komentarza przed dostępem	Audyt intencji użytkownika	Użytkownik musi wpisać uzasadnienie, zanim uzyska dostęp do punktu końcowego
13	Integracja z Active Directory	Centralne zarządzanie tożsamościami	System pozwala na logowanie i synchronizację kont z usługą AD
14	Integracja z SIEM	Możliwość przesyłania logów i alertów	System wysyła zdarzenia do zewnętrznych systemów analizy bezpieczeństwa (SIEM)
15	Rejestrowanie online/offline klienta do SIEM	Informacja o statusie agenta w czasie rzeczywistym	System loguje przełączenia trybu online/offline agenta i eksportuje dane do SIEM
16	Integracja z WebLogin	Zewnętrzne logowanie do systemu PAM	System wspiera mechanizmy logowania przez zewnętrzne portale SSO
17	Integracja z SAML	Federacyjne uwierzytelnianie	Możliwość integracji z usługami tożsamości wspierającymi SAML 2.0
18	Integracja z OneLogin (SAML)	SSO z OneLogin	System obsługuje SAML jako metodę logowania do platformy
19	Integracja z Okta (SAML)	Federacja tożsamości z Okta	Możliwość podłączenia PAM do Okta jako dostawcy tożsamości
20	Ograniczenie dostępu wg czasu pracy	Kontrola godzinowa logowania	System może uniemożliwić logowanie poza ustalonym harmonogramem godzin pracy

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
21	Integracja z serwerem certyfikatów	Dodatkowe zatwierdzanie żądań dostępu	Możliwość wystawienia certyfikatu przez CA jako wymóg dla uruchomienia sesji
22	Widok jednej strony dla żądań dostępu	Ułatwienie pracy administratora	Interfejs pozwala przeglądać i zatwierdzać żądania OTP, dostępu USB, końcówek itd. w jednym miejscu
23	Wykrywanie nietypowych zachowań użytkownika	System analizuje wzorce pracy w czasie rzeczywistym	Wbudowany moduł UEBA umożliwia identyfikację anomalii i podejrzanych działań
24	Ochrona dziennika audytu	Zapobieganie modyfikacjom logów	System uniemożliwia manipulowanie logami audytu, nawet użytkownikom uprzywilejowanym

5.3.6. Produktywność i Raportowanie

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Eksport danych statystycznych do formatów xlsx/xls	Możliwość zapisania wyników monitoringu do Excela	System umożliwia eksport danych z raportów do plików xlsx/xls bezpośrednio z interfejsu
2	Pulpity produktywności	Graficzne przedstawienie aktywności użytkowników i ich wydajności	System oferuje predefiniowane widoki produktywności – np. czas aktywności, używane aplikacje

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
3	Wbudowany silnik raportowania	Generowanie raportów wg wielu parametrów, bez potrzeby zewnętrznych narzędzi	Wbudowany moduł raportowania umożliwia filtrowanie wg użytkownika, czasu, aplikacji, działań
4	Tworzenie raportów według harmonogramu	Automatyzacja cyklicznego generowania raportów	System umożliwia ustawienie harmonogramów do codziennego, tygodniowego lub miesięcznego raportowania
5	Integracja z Power BI	Eksport danych do narzędzia BI	Możliwość połączenia systemu z Power BI przez API lub eksport danych do formatów akceptowanych przez BI
6	Szablony eksportu dla Microsoft Power BI	Gotowe wzory danych do analizy w BI	System zawiera gotowe zestawy pól i struktur danych do łatwego użycia w Power BI
7	Analiza częstotliwości użycia aplikacji i stron	Monitoring wykorzystania zasobów IT	System mierzy, jak długo i jak często aplikacje oraz strony są wykorzystywane przez użytkowników
8	Zarządzanie problemami serwera centralnego i bazy danych z powiadomieniami e-mail	Monitoring kondycji infrastruktury systemu	System nadzoruje zużycie zasobów, przestrzeń dyskową i inne parametry – z powiadomieniami o problemach
9	Możliwość dostosowywania raportów	Personalizacja układu, zawartości i filtrów raportów	Administrator może tworzyć własne szablony raportów, wybierać kolumny, grupowania i formaty

5.3.7. Zarządzanie hasłami

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Zarządzanie hasłami do Windows Server, Linux, systemów webowych, MS SQL Server, Active Directory	System powinien centralnie zarządzać hasłami do różnych systemów operacyjnych i usług	Moduł PAM pozwala na bezpieczne przechowywanie, rotację i używanie haseł do wymienionych systemów
2	Selektywne rejestrowanie aktywności tylko dla uprzywilejowanych użytkowników	Ograniczenie nagrywania do użytkowników o podwyższonych uprawnieniach	System pozwala na wybranie, którzy użytkownicy będą objęci monitoringiem w module PAM
3	Tworzenie listy dozwolonych punktów końcowych do użycia sekretów	Kontrola lokalizacji, z których można uzyskiwać dostęp do wrażliwych danych	Lista punktów końcowych pozwala ograniczyć użycie haseł do zaufanych hostów
4	Wykrywanie lokalnych uprzywilejowanych kont Windows	Automatyczne znajdowanie kont z uprawnieniami administratora	System skanuje hosty i identyfikuje konta z uprawnieniami admina lokalnego
5	Wykrywanie uprzywilejowanych kont Active Directory	Identyfikacja i rejestracja kont domenowych z podwyższonymi prawami	System automatycznie znajduje i kategoryzuje konta AD jako uprzywilejowane
6	Wprowadzanie wykrytych kont do sekretów masowo	Automatyczne dodawanie kont do repozytorium haseł	Administrator może jednym kliknięciem dodać wiele kont do systemu zarządzania hasłami

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Reguły automatycznego wykrywania kont uprzywilejowanych	Definiowanie warunków wykrywania np. nazwy grup, ról	System umożliwia konfigurację detekcji kont wg ról, grup lub lokalizacji
8	Zdalna rotacja haseł	Możliwość zmiany haseł bez fizycznego dostępu do urządzenia	System pozwala rotować hasła kont zdalnie w cyklach lub na żądanie
9	Nawigacja do sekretu i powiązanych sesji	Szybkie odnajdywanie użycia haseł	Funkcja umożliwia znalezienie każdej sesji, w której użyto danego sekretu
10	Obsługa żądań dostępu do sekretów z wyborem typu dostępu	Kontrola nad tym, kto i jak może użyć danego hasła	System umożliwia ustawienie typów dostępu: tylko podgląd, sesja pośrednia, pobranie itd.
11	Broker poświadczeń aplikacji	Umożliwia integrację z aplikacjami wymagającymi haseł	System działa jako pośrednik przekazujący poświadczenia bez ich ujawniania użytkownikowi
12	Zarządzanie hasłami osobistymi	Możliwość używania rozwiązań także przez indywidualnych użytkowników	Użytkownicy mogą przechowywać i zarządzać własnymi danymi dostępowymi w ramach systemu
13	Przesyłanie plików w ramach procedur zarządzania hasłami	Bezpieczne zarządzanie operacjami plikowymi przez PAM	System umożliwia przekazywanie plików w kontekście sesji z użyciem danego sekretu lub konta

5.3.8. Szkolenia

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Podstawy	Znajomość działania i komponentów systemu	Kurs wprowadzający online
2	Instalacja i konfiguracja	Umiejętność wdrożenia systemu	Warsztaty praktyczne
3	Zgodność i raportowanie	Monitorowanie zgodności z normami (np. GDPR)	Szkolenie tematyczne
4	Forma zdalna	Szkolenie nie wymaga obecności fizycznej uczestników.	Warsztaty prowadzone online przy użyciu komunikatora uzgodnionego z Zamawiającym.
5	Materiały szkoleniowe w języku polskim	Uczestnicy powinni mieć dostęp do materiałów edukacyjnych.	Wykonawca dostarcza elektroniczne materiały szkoleniowe w języku polskim (PDF, prezentacje).
6	Uzgodnienie szczegółowego planu i terminów z Zamawiającym	Terminy i zakres powinny odpowiadać potrzebom organizacyjnym Zamawiającego.	Wykonawca uzgadnia harmonogram i agendę warsztatów z przedstawicielem Zamawiającego przed realizacją.

5.4. Wymagania dla Web Application Firewall (SaaS)

5.4.1. Licencjonowanie

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1.	Licencja na poziomie jednej domeny	Każdy plan obejmuje tylko jedną domenę, co oznacza, że licencja nie może być współdzielona przez wiele domen.	Licencja przypisana do jednej domeny, dodawana do konta użytkownika z pełnym dostępem do funkcji planu dla tej domeny.
2.	Wybór poziomu subskrypcji przy dodawaniu domeny	System powinien umożliwiać wybór planu dla każdej dodawanej domeny, aby administrator mógł dopasować funkcje do wymagań domeny.	Panel administracyjny z opcją przypisania planu do każdej domeny przy jej dodaniu lub zmianie poziomu subskrypcji.
3.	Powiadomienia o terminie wygaśnięcia licencji	System powinien informować administratora o zbliżającym się terminie wygaśnięcia planu dla każdej domeny, aby uniknąć przerwania usług.	Automatyczne powiadomienie e-mail wysyłane 30 dni przed datą wygaśnięcia subskrypcji.
4.	Odnowienie subskrypcji	System powinien umożliwiać automatyczne odnowienie subskrypcji, aby zapewnić ciągłość działania usług dla przypisanej domeny.	Automatyczne obciążenie karty płatniczej na koniec okresu rozliczeniowego i przedłużenie subskrypcji bez przestojów.
5.	Przypisanie płatności do konkretnej domeny	Każda płatność za plan powinna być przypisana do wybranej domeny, co zapewnia, że funkcje są dostępne wyłącznie dla tej domeny.	Płatność przypisywana bezpośrednio do subskrypcji wybranej domeny z pełnym dostępem do funkcji planu tylko dla tej domeny.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
6.	Przegląd historii subskrypcji dla domen	System powinien umożliwiać administratorowi przegląd historii subskrypcji dla każdej domeny, w tym dat rozpoczęcia i zakończenia licencji.	Moduł historii licencji w panelu administracyjnym z informacjami o wszystkich poprzednich i bieżących subskrypcjach.
7.	Zgodność z regulacjami dotyczącymi płatności online	System powinien zapewniać zgodność z regulacjami dotyczącymi płatności online, aby zabezpieczyć transakcje za subskrypcję.	Obsługa płatności zgodnie z PCI-DSS, zapewniająca bezpieczne przetwarzanie płatności za subskrypcje Pro w systemie.

5.4.2. Zabezpieczenia aplikacji internetowych

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Ochrona przed atakami DDoS	System powinien automatycznie wykrywać i blokować ataki DDoS na poziomie aplikacji, aby zapewnić nieprzerwane działanie aplikacji.	Zintegrowana zaporą sieciową wykrywająca i blokująca nadmierny ruch bez opóźnienia w dostępie dla legalnych użytkowników.
2	WAF (Web Application Firewall) z regułami OWASP	System powinien zapewniać ochronę przed popularnymi typami ataków (np. SQL Injection, XSS), zgodnie z regułami OWASP.	Web Application Firewall z regułami OWASP blokujący popularne techniki ataków na poziomie aplikacji.
3	Filtracja adresów IP	System powinien umożliwiać administratorowi blokowanie lub dopuszczanie ruchu na podstawie list adresów IP.	Funkcja zarządzania listami IP w zaporze, z możliwością ręcznego dodawania lub blokowania określonych adresów.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
4	Podstawowa ochrona przed botami	System powinien rozpoznawać i ograniczać działanie botów, aby zapobiec przeciążeniu aplikacji.	Proste mechanizmy rozpoznawania botów w oparciu o analizę wzorców ruchu i ograniczenia dostępu.
5	Automatyczna aktualizacja bazy zagrożeń	System powinien automatycznie aktualizować reguły bezpieczeństwa i ochrony przed atakami w oparciu o bazę danych Cloudflare.	Automatyczne aktualizacje reguł ochrony i bazy zagrożeń bez konieczności ręcznej konfiguracji.
6	Obsługa SSL/TLS	System powinien umożliwiać administratorowi zarządzanie certyfikatami SSL/TLS, aby zapewnić szyfrowane połączenia z aplikacją.	Możliwość generowania i zarządzania certyfikatami SSL bezpośrednio w panelu administracyjnym.
7	Force HTTPS	System powinien wymuszać korzystanie z protokołu HTTPS, aby zapewnić bezpieczne połączenia dla użytkowników.	Funkcja przekierowania z HTTP na HTTPS, włączana w panelu administratora.
8	Zarządzanie certyfikatami przez Cloudflare	System powinien automatycznie odnawiać certyfikaty SSL, aby uniknąć przerwania bezpiecznych połączeń.	Automatyczne odnawianie certyfikatów zarządzanych przez Cloudflare.
9	Obsługa protokołów HTTP/2 i HTTP/3	System powinien obsługiwać nowoczesne protokoły HTTP/2 i HTTP/3, aby przyspieszyć ładowanie strony.	Automatyczne wdrożenie i optymalizacja protokołów HTTP/2 i HTTP/3 dla przyspieszenia połączeń.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
10	Raportowanie o zagrożeniach i atakach	System powinien dostarczać raporty na temat wykrytych zagrożeń i ataków, aby administrator mógł analizować incydenty.	Generowanie raportów dostępnych w panelu administracyjnym, obejmujących liczbę i typ wykrytych zagrożeń.

5.4.3. Optymalizacja wydajności aplikacji internetowych

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Cache'owanie zasobów statycznych	System powinien automatycznie cache'ować statyczne zasoby aplikacji, aby przyspieszyć czas ładowania strony.	Automatyczne cache'owanie plików takich jak obrazy, CSS i JavaScript na serwerach Cloudflare z możliwością konfiguracji TTL.
2	Optymalizacja obrazów z konwersją do WebP	System powinien konwertować obrazy do formatu WebP, aby zmniejszyć ich rozmiar i przyspieszyć ładowanie strony na przeglądarkach obsługujących WebP.	Moduł automatycznej konwersji obrazów na format WebP dla szybszego ładowania i zmniejszenia zużycia przepustowości.
3	Kompresja plików	System powinien kompresować pliki przesyłane pomiędzy serwerem a przeglądarką, aby zmniejszyć ich rozmiar.	Automatyczna kompresja gzip lub brotli dla plików tekstowych, takich jak CSS i JavaScript.
4	Obsługa HTTP/2 i HTTP/3	System powinien automatycznie obsługiwać HTTP/2 i HTTP/3, co pozwala przyspieszyć ładowanie	Włączenie HTTP/2 i HTTP/3 dla wszystkich zasobów strony, co poprawia szybkość i efektywność

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		strony poprzez lepsze zarządzanie połączeniami.	Ładowania w przeglądarkach wspierających te protokoły.
5	Funkcja Polish do optymalizacji obrazów	System powinien oferować funkcję Polish, która automatycznie kompresuje obrazy bez widocznej utraty jakości.	Automatyczna kompresja obrazów z możliwością aktywacji funkcji Polish w panelu Cloudflare.
6	Prefetching DNS	System powinien oferować prefetching DNS dla zewnętrznych zasobów, aby zmniejszyć czas ich ładowania.	Wstępne pobieranie danych DNS, które przyspiesza ładowanie zasobów spoza domeny głównej.
7	Optymalizacja zasobów CSS i JavaScript	System powinien automatycznie optymalizować pliki CSS i JavaScript poprzez usuwanie zbędnych danych i kompresję.	Minifikacja CSS i JavaScript, która usuwa niepotrzebne spacje i komentarze, zmniejszając rozmiar plików.
8	Globalna sieć CDN	System powinien korzystać z globalnej sieci CDN, aby przyspieszyć dostarczanie treści do użytkowników z różnych regionów.	Dystrybucja treści przez serwery Cloudflare znajdujące się w różnych lokalizacjach na całym świecie.
9	Automatyczne dostosowanie cache'owania do ruchu	System powinien automatycznie dostosowywać poziom cache'owania na podstawie wzorców ruchu użytkowników.	Adaptacyjne cache'owanie oparte na analizie intensywności ruchu i dostosowane do lokalnych zasobów.
10	Raportowanie o efektywności cache'owania	System powinien dostarczać raporty o skuteczności cache'owania, aby administrator mógł analizować, które zasoby wymagają optymalizacji.	Raporty cache hit/miss, które informują o skuteczności przechowywania zasobów w pamięci podręcznej.

5.4.4. Ochrona przed botami

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Weryfikacja CAPTCHA	System powinien stosować mechanizmy CAPTCHA w celu ograniczenia dostępu botów i zapewnienia dostępności aplikacji dla legalnych użytkowników.	Weryfikacja CAPTCHA dla żądań rozpoznanych jako podejrzone lub generowanych przez boty.
2	Podstawowa analiza ruchu botów	System powinien identyfikować boty na podstawie wzorców ruchu, aby blokować nadmiarowy ruch z nieautoryzowanych źródeł.	Analiza ruchu użytkowników na podstawie zidentyfikowanych wzorców zachowania, takich jak wielokrotne żądania w krótkim czasie.
3	Dynamiczne dostosowanie blokady botów	System powinien dynamicznie dostosowywać poziom blokady ruchu botów w zależności od natężenia ruchu.	Skalowanie blokady w oparciu o bieżący ruch i wzorce działania botów.
4	Integracja ochrony botów z WAF	System powinien integrować mechanizmy ochrony przed botami z zaporą aplikacyjną (WAF), aby zapewnić kompleksową ochronę przed złośliwym ruchem.	Połączenie ochrony botów z regułami WAF, co umożliwia blokowanie ruchu generowanego przez boty oraz nietypowych zapytań.
5	Monitorowanie aktywności botów	System powinien monitorować działania wykrytych botów w czasie rzeczywistym, aby administrator mógł analizować zagrożenia.	Moduł monitorowania, który wyświetla raporty o aktywności botów oraz podjętych działaniach ochronnych.
6	Zgłaszanie nietypowych botów	System powinien umożliwiać administratorowi zgłaszanie	Funkcja zgłaszania nietypowych botów, co umożliwia Cloudflare aktualizację i poprawę ochrony.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		nowych botów, które omijają standardowe mechanizmy ochrony.	

5.4.5. Optymalizacja SEO i prędkości ładowania strony

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Automatyczna optymalizacja obrazów pod kątem SEO	System powinien optymalizować obrazy (np. kompresować) dla szybszego ładowania, co wpływa na ranking SEO w wyszukiwarkach.	Moduł kompresji i optymalizacji obrazów, który poprawia prędkość ładowania zasobów bez utraty jakości.
2	Obsługa HTTP/2 i HTTP/3 dla lepszego SEO	System powinien automatycznie obsługiwać protokoły HTTP/2 i HTTP/3, które są preferowane przez wyszukiwarki i wspierają lepsze SEO.	Automatyczne włączenie HTTP/2 i HTTP/3, co poprawia szybkość ładowania i wpływa pozytywnie na pozycjonowanie.
3	Minimalizacja plików CSS i JavaScript	System powinien automatycznie usuwać zbędne elementy z plików CSS i JavaScript, aby przyspieszyć ładowanie strony.	Funkcja minifikacji plików, która usuwa spacje, komentarze i inne niepotrzebne dane z kodu CSS/JS.
4	Prefetching zasobów DNS	System powinien umożliwiać prefetching DNS dla zasobów zewnętrznych, aby zmniejszyć czas ładowania strony.	Moduł prefetchingu, który pobiera informacje DNS o zasobach zewnętrznych zanim zostaną użyte przez użytkownika.
5	Automatyczne dostosowanie	System powinien automatycznie dostosowywać rozdzielczość obrazów w zależności od	Funkcja dostosowania rozdzielczości, która optymalizuje obrazy dla

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
	rozdzielczości obrazów	urządzenia, co wpływa na szybkość ładowania.	przeglądarek mobilnych i stacjonarnych.
6	Generowanie raportów o prędkości ładowania	System powinien dostarczać administratorowi raporty o prędkości ładowania, aby mógł analizować i optymalizować wydajność strony.	Automatyczne raportowanie metryk prędkości ładowania strony z możliwością przeglądu i eksportu danych.

5.4.6. Szkolenia

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Podstawy	Znajomość działania i komponentów systemu	Kurs wprowadzający online
2	Instalacja i konfiguracja	Umiejętność wdrożenia systemu	Warsztaty praktyczne
3	Reguły i alerty	Tworzenie i zarządzanie regułami bezpieczeństwa	Kurs zaawansowany
4	Forma zdalna	Szkolenie nie wymaga obecności fizycznej uczestników.	Warsztaty prowadzone online przy użyciu komunikatora uzgodnionego z Zamawiającym.

5	Materiały szkoleniowe w języku polskim	Uczestnicy powinni mieć dostęp do materiałów edukacyjnych.	Wykonawca dostarcza elektroniczne materiały szkoleniowe w języku polskim (PDF, prezentacje).
6	Uzgodnienie szczegółowego planu i terminów z Zamawiającym	Terminy i zakres powinny odpowiadać potrzebom organizacyjnym Zamawiającego.	Wykonawca uzgadnia harmonogram i agendę warsztatów z przedstawicielem Zamawiającego przed realizacją.

5.5. Wymagania dla System Information and Event Management

5.5.1. Zarządzanie logami i analiza zdarzeń

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Obsługa różnorodnych źródeł logów	System powinien gromadzić logi z różnych urządzeń, aplikacji, baz danych i systemów operacyjnych.	Wsparcie dla formatów syslog, JSON, XML oraz możliwość integracji przez API do pobierania logów z różnych systemów.
2	Centralne przechowywanie logów	System powinien umożliwiać centralne przechowywanie wszystkich logów dla ułatwienia analizy i audytu.	Baza danych na serwerze on-premise przechowująca logi z dostępem do przeglądu przez panel administracyjny.
3	Wyszukiwanie i filtrowanie logów	System powinien umożliwiać szybkie przeszukiwanie i filtrowanie logów według parametrów, takich jak czas, źródło, typ.	Mechanizm indeksowania logów oraz panel do definiowania i wykonywania zaawansowanych zapytań wyszukiwania.
4	Zachowanie integralności logów	System powinien zapewniać, że zebrane logi nie będą modyfikowane ani usuwane bez odpowiednich uprawnień.	Funkcja kontroli dostępu oraz rejestracja wszelkich modyfikacji lub prób modyfikacji w oddzielnym logu audytowym.
5	Obsługa dużych wolumenów danych	System powinien obsługiwać duże ilości danych i działać wydajnie nawet przy wysokim natężeniu logów.	Skalowalna architektura umożliwiająca rozbudowę zasobów przechowywania i mocy przetwarzania w razie potrzeby.
6	Wykrywanie korelacji między zdarzeniami	System powinien wykrywać zależności między różnymi zdarzeniami logów w celu identyfikacji potencjalnych zagrożeń.	Moduł korelacji, który analizuje wzorce i sekwencje zdarzeń, generując alerty na podstawie zdefiniowanych reguł.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Oznaczanie i klasyfikacja zdarzeń	System powinien klasyfikować zdarzenia według priorytetu i rodzaju zagrożenia, aby ułatwić ich analizę.	Automatyczna klasyfikacja zdarzeń na podstawie typów logów i zdefiniowanych polityk klasyfikacji.
8	Tworzenie alertów na podstawie logów	System powinien generować alerty o potencjalnych zagrożeniach wykrytych w logach i przekazywać je do administratora.	Moduł alertowania, który wysyła powiadomienia e-mail lub SMS przy wykryciu zdarzeń zgodnych z regułami alertów.
9	Retencja danych	System powinien umożliwiać konfigurację okresu przechowywania logów zgodnie z wymogami regulacyjnymi.	Konfigurowalna polityka retencji, która automatycznie usuwa logi po upływie określonego okresu.
10	Eksport logów do formatu CSV lub PDF	System powinien umożliwiać eksport danych logów do formatów takich jak CSV lub PDF w celu dalszej analizy lub raportowania.	Opcja eksportu logów z panelu administracyjnego z możliwością wyboru zakresu czasowego i innych parametrów.
11	Przesyłanie alertów do SOC	System powinien mieć wbudowaną funkcję, która przesyła alerty do zdalnego SOC wraz z próbkami danych, która te alerty wywołała.	Dane przesyłane są w połączeniu szyfrowanych do przypisanej do klienta przestrzeni SOC, bezpośrednio na pulpit inżyniera.

5.5.2. Zarządzanie incydentami i odpowiedź na zagrożenia

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Tworzenie i zarządzanie incydentami	System powinien umożliwiać tworzenie i zarządzanie incydentami na podstawie wykrytych zdarzeń lub zgłoszeń użytkowników.	Moduł zarządzania incydentami z opcjami dodawania, aktualizacji oraz monitorowania statusu incydentów.
2	Automatyczna eskalacja incydentów	System powinien automatycznie eskalować incydenty o wysokim priorytecie do wyższych poziomów wsparcia.	Definiowanie reguł eskalacji incydentów, które automatycznie przypisują je do kolejnych poziomów wsparcia.
3	Powiadamianie o incydentach	System powinien wysyłać powiadomienia o wykrytych incydentach do odpowiednich osób w celu szybkiego reagowania.	Konfigurowalne powiadomienia e-mail i SMS na podstawie priorytetu incydentu oraz przypisanych użytkowników.
4	Tworzenie zadań związanych z incydentami	System powinien umożliwiać przypisywanie zadań poszczególnym użytkownikom w celu szybkiego rozwiązania incydentów.	Moduł zarządzania zadaniami z opcjami przydzielania zadań do incydentów oraz monitorowania ich statusu.
5	Dokumentacja incydentów	System powinien umożliwiać dodawanie notatek i dokumentacji do incydentów, aby śledzić kroki podjęte w celu ich rozwiązania.	Sekcja komentarzy i załączników do każdego incydentu, umożliwiająca dokumentowanie działań i wyników.
6	Integracja z systemami zewnętrznymi	System powinien integrować się z innymi systemami bezpieczeństwa, aby	API do integracji z innymi narzędziami bezpieczeństwa oraz możliwość eksportu danych do systemów SIEM i SOAR.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		automatyzować wykrywanie i reakcję na zagrożenia.	
7	Analiza pierwotnej przyczyny	System powinien wspierać analizę przyczyn incydentów, aby zidentyfikować źródło zagrożenia i zapobiec jego powtórzeniu.	Moduł analizy przyczyn z dostępem do historii logów oraz raportów korelacyjnych związanych z incydemem.
8	Raportowanie incydentów	System powinien generować raporty incydentów z informacjami o rodzaju, przyczynie i podjętych działaniach.	Automatyczne raportowanie incydentów z możliwością eksportu do formatu PDF oraz podglądem historii incydentów.
9	Automatyczna klasyfikacja incydentów	System powinien klasyfikować incydenty na podstawie ich priorytetu, typu i źródła, aby ułatwić analizę i rozwiązanie.	Moduł klasyfikacji incydentów na podstawie reguł ustalonych przez administratora.
10	Możliwość tworzenia szablonów reakcji na incydenty	System powinien oferować gotowe szablony reakcji na najczęstsze rodzaje incydentów, aby przyspieszyć działania zespołu.	Opcja definiowania i wykorzystywania szablonów reakcji w zależności od klasyfikacji i rodzaju incydentu.

5.5.3. Automatyzacja i zarządzanie regułami

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Automatyzacja działań w odpowiedzi na incydenty	System powinien automatyzować określone działania w odpowiedzi na	Moduł automatyzacji, który uruchamia zdefiniowane akcje

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		incydenty, aby zmniejszyć czas reakcji na zagrożenia.	(np. blokowanie IP) w reakcji na określone incydenty.
2	Tworzenie reguł korelacyjnych	System powinien umożliwiać tworzenie reguł korelacji między różnymi typami zdarzeń w celu wykrywania zagrożeń.	Interfejs do definiowania reguł korelacji z wyborem różnych parametrów zdarzeń oraz alertów.
3	Harmonogramowanie raportów	System powinien pozwalać na automatyczne generowanie raportów w określonych odstępach czasu (np. tygodniowe, miesięczne).	Funkcja harmonogramowania raportów z opcją dostosowania interwałów czasowych i formatu raportu.
4	Automatyczne aktualizacje bazy zagrożeń	System powinien regularnie aktualizować bazę zagrożeń, aby zapewnić ochronę przed najnowszymi rodzajami ataków.	Funkcja automatycznej aktualizacji baz zagrożeń poprzez integrację z zewnętrznymi źródłami danych o zagrożeniach.
5	Tworzenie szablonów automatyzacji	System powinien oferować możliwość tworzenia i zarządzania szablonami automatyzacji dla standardowych działań.	Moduł szablonów automatyzacji, który umożliwia definiowanie działań i reguł wykonania w zależności od scenariuszy.
6	Reagowanie na anomalie	System powinien identyfikować anomalie w ruchu sieciowym i automatycznie podejmować działania zapobiegawcze.	Algorytm wykrywający anomalie oraz reguły inicjujące reakcje (np. blokada) na podstawie ustalonych progów.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
7	Automatyczne przypisywanie incydentów	System powinien automatycznie przypisywać incydenty do odpowiednich członków zespołu na podstawie zdefiniowanych reguł.	Moduł zarządzania incydentami z opcją przypisania na podstawie roli i dostępności personelu.
8	Przetwarzanie zdarzeń w czasie rzeczywistym	System powinien przetwarzać zdarzenia i podejmować decyzje w czasie rzeczywistym, aby natychmiast reagować na zagrożenia.	Mechanizm analizy i reagowania na logi oraz zdarzenia w czasie rzeczywistym z automatycznym generowaniem alertów.
9	Reguły blokowania ruchu sieciowego	System powinien umożliwiać automatyczne blokowanie określonych typów ruchu sieciowego w reakcji na incydenty.	Interfejs konfiguracji blokady ruchu na poziomie IP lub portu na podstawie ustalonych reguł.
10	Integracja z narzędziami SIEM	System powinien integrować się z systemami SIEM w celu wymiany danych i raportowania incydentów.	API do integracji oraz eksportu zdarzeń i incydentów do zewnętrznych systemów SIEM.

5.5.4. Rozszerzone funkcje analizy zagrożeń i automatyzacji

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Integracja z narzędziami Threat Intelligence	System powinien automatycznie pobierać dane o zagrożeniach z zewnętrznych źródeł Threat Intelligence i wykorzystywać je do analizy incydentów.	Mechanizm integracji z platformami Threat Intelligence, które regularnie aktualizują bazę zagrożeń.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
2	Uczenie maszynowe do wykrywania wzorców	System powinien wykorzystywać modele uczenia maszynowego do wykrywania nietypowych wzorców w ruchu sieciowym i zachowaniu użytkowników.	Moduł analityczny oparty na ML, analizujący dane historyczne i na bieżąco identyfikujący anomalie.
3	Analiza behawioralna	System powinien analizować zachowania użytkowników i urządzeń w sieci, aby wykrywać nietypowe działania.	Moduł analizy behawioralnej, który porównuje bieżące działania z ustalonymi profilami normalnych zachowań.
4	Ochrona przed atakami Zero-Day	System powinien mieć mechanizmy wykrywania i reagowania na zagrożenia zero-day.	Funkcje analizujące nietypowe wzorce działań i wykorzystujące Threat Intelligence do oceny nieznanych zagrożeń.
5	Zarządzanie ryzykiem na podstawie oceny incydentów	System powinien oceniać ryzyko na podstawie analizy zgłoszonych incydentów i ustalać priorytety działań w oparciu o poziom ryzyka.	Moduł zarządzania ryzykiem, który przypisuje incydom oceny ryzyka na podstawie ich wpływu i prawdopodobieństwa.
6	Automatyczne przypisanie zasobów	System powinien automatycznie przydzielać zasoby (np. personel, narzędzia) do reakcji na incydenty o wysokim priorytecie.	Algorytm przypisujący zadania zespołom i administratorom na podstawie dostępności oraz specjalizacji.
7	Raportowanie zgodności z wymaganiami regulacyjnymi	System powinien generować raporty zgodności z przepisami, takimi jak RODO, NIS2 lub PCI-DSS, na podstawie zgromadzonych danych.	Moduł raportowania zgodności z opcją eksportu danych w formatach PDF i CSV.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
8	Moduł SOAR (Security Orchestration, Automation and Response)	System powinien umożliwiać pełną automatyzację odpowiedzi na incydenty bezpieczeństwa przy użyciu predefiniowanych workflow.	Interfejs do tworzenia i edycji workflow automatyzujących procesy wykrywania i odpowiedzi na incydenty.
9	Identyfikacja zagrożeń na podstawie analizy anomalii	System powinien wykrywać nietypowe zachowania użytkowników, urządzeń i sieci, które mogą sugerować atak.	Moduł analizy anomalii z możliwością automatycznego generowania alertów na podstawie odchyłeń od normy.
10	Automatyczne blokowanie ruchu sieciowego na podstawie reguł	System powinien automatycznie blokować złośliwy ruch sieciowy na podstawie predefiniowanych reguł i analizy ryzyka.	Moduł automatycznego reagowania, który identyfikuje zagrożenia i podejmuje akcje blokujące w czasie rzeczywistym.

5.5.5. Rozszerzone funkcje raportowania i monitorowania zgodności

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Generowanie raportów z harmonogramem	System powinien umożliwiać planowanie generowania raportów zgodności w ustalonych odstępach czasu (np. kwartalnie).	Harmonogramowanie raportów z możliwością wyboru częstotliwości oraz zakresu raportowanych danych.
2	Raportowanie zgodności z NIS2	System powinien generować raporty zgodności z wytycznymi dyrektywy NIS2 dla infrastruktury krytycznej.	Automatyczny generator raportów zgodności z NIS2 na podstawie zebranych danych operacyjnych i incydentów.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
3	Tworzenie audytów bezpieczeństwa	System powinien umożliwiać tworzenie i zarządzanie audytami bezpieczeństwa dla różnych zasobów organizacji.	Moduł do tworzenia audytów z przypisanymi zadaniami i możliwością dokumentowania wyników oraz rekomendacji.
4	Analiza trendów w incydentach	System powinien umożliwiać analizę trendów incydentów w celu identyfikacji najczęściej występujących zagrożeń.	Funkcja raportowania trendów incydentów z możliwością filtrowania według typu, źródła i priorytetu.
5	Zarządzanie politykami zgodności	System powinien oferować moduł do zarządzania politykami zgodności, umożliwiając tworzenie, edycję i monitorowanie ich przestrzegania.	Interfejs do zarządzania politykami zgodności z możliwością przypisania ich do użytkowników i zasobów.
6	Raporty dla interesariuszy i audytorów	System powinien umożliwiać tworzenie raportów dostosowanych do potrzeb audytorów i interesariuszy, takich jak zarząd.	Moduł generowania raportów z predefiniowanymi szablonami dla audytów wewnętrznych i zewnętrznych.
7	Zgodność z wytycznymi PCI-DSS	System powinien umożliwiać monitorowanie i raportowanie zgodności z wytycznymi PCI-DSS dla danych płatniczych.	Moduł monitorowania zgodności PCI-DSS z powiadomieniami o wszelkich niezgodnościach z wymaganiami standardu.
8	Integracja z systemami GRC	System powinien integrować się z narzędziami do zarządzania ryzykiem i zgodnością (GRC) w celu automatycznego przesyłania danych.	API umożliwiające wymianę informacji o incydentach i zgodności z narzędziami GRC.

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
9	Automatyczne powiadomienia o niezgodnościach	System powinien automatycznie powiadamiać o wykrytych niezgodnościach z politykami bezpieczeństwa i wymogami regulacyjnymi.	Funkcja alertów dla administratorów przy wykryciu niezgodności z politykami lub regulacjami.
10	Generowanie raportów na żądanie	System powinien umożliwiać generowanie raportów zgodności na żądanie, dostosowanych do bieżących potrzeb audytowych.	Opcja generowania niestandardowych raportów na żądanie z dostosowanymi filtrami i parametrami.

5.5.6. Rozszerzone funkcje monitorowania operacyjnego i automatyzacji operacji

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Pełna widoczność ruchu sieciowego	System powinien umożliwiać pełne monitorowanie ruchu sieciowego, identyfikując nieautoryzowane próby dostępu i anomalie.	Moduł do monitorowania ruchu sieciowego, który analizuje pakiety i generuje alerty przy wykryciu anomalii.
2	Automatyczne reagowanie na zdarzenia krytyczne	System powinien automatycznie podejmować działania w przypadku wykrycia zdarzeń krytycznych, aby minimalizować ich wpływ.	Funkcja definiowania akcji reakcji na zdarzenia krytyczne, np. odcięcie zasobów lub zablokowanie kont użytkowników.
3	Monitorowanie aktywności użytkowników	System powinien monitorować działania użytkowników w czasie rzeczywistym, aby	Moduł analizy aktywności użytkowników z opcją

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		identyfikować podejrzone aktywności.	alertowania przy wykryciu nieautoryzowanych działań.
4	Automatyczne skalowanie zasobów w czasie wzmożonego ruchu	System powinien automatycznie skalować zasoby przetwarzania danych w przypadku wzrostu natężenia ruchu.	Mechanizm automatycznego przydzielania zasobów serwera na podstawie analizy obciążenia i aktywności w sieci.
5	Przechowywanie danych do analizy retrospektywnej	System powinien przechowywać dane przez określony czas, aby umożliwić analizę retrospektywną incydentów i anomalii.	Archiwizacja danych logów i incydentów na serwerze on-premise z ustalonym okresem przechowywania.
6	Wsparcie dla kontroli dostępu opartej na rolach	System powinien umożliwiać nadawanie uprawnień użytkownikom na podstawie ich roli w organizacji, aby ograniczyć dostęp.	Moduł kontroli dostępu, który przypisuje prawa dostępu na podstawie ról i polityk organizacyjnych.
7	Integracja z narzędziami do zarządzania tożsamością i dostępem (IAM)	System powinien wspierać integrację z systemami IAM w celu synchronizacji uprawnień użytkowników.	API do integracji z narzędziami IAM, które automatycznie synchronizują polityki dostępu użytkowników.
8	Wizualizacja stanu bezpieczeństwa w czasie rzeczywistym	System powinien oferować dashboard do wizualizacji stanu bezpieczeństwa i aktywności w czasie rzeczywistym.	Panel nawigacyjny z widokiem kluczowych wskaźników bezpieczeństwa i monitorowania incydentów.
9	Identyfikacja i raportowanie zagrożeń na poziomie plików	System powinien monitorować i raportować zagrożenia wykryte na poziomie dostępu do plików,	Moduł do monitorowania dostępu do plików i dokumentów z opcją alertów

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
		aby zabezpieczyć wrażliwe dane.	przy wykryciu podejrzanych działań.
10	Integracja z narzędziami do archiwizacji	System powinien integrować się z narzędziami do archiwizacji danych, aby zapewnić długoterminowe przechowywanie logów i raportów.	Opcja eksportu logów i incydentów do zewnętrznych systemów archiwizacji.

5.5.7. Szkolenia

Lp.	Wymaganie	Wyjaśnienie	Sposób spełnienia
1	Podstawy	Znajomość działania i komponentów systemu	Kurs wprowadzający online
2	Instalacja i konfiguracja	Umiejętność wdrożenia systemu	Warsztaty praktyczne
3	Reguły i alerty	Tworzenie i zarządzanie regułami bezpieczeństwa	Kurs zaawansowany
4	Forma zdalna	Szkolenie nie wymaga obecności fizycznej uczestników.	Warsztaty prowadzone online przy użyciu komunikatora uzgodnionego z Zamawiającym.

5	Materiały szkoleniowe w języku polskim	Uczestnicy powinni mieć dostęp do materiałów edukacyjnych.	Wykonawca dostarcza elektroniczne materiały szkoleniowe w języku polskim (PDF, prezentacje).
6	Uzgodnienie szczegółowego planu i terminów z Zamawiającym	Terminy i zakres powinny odpowiadać potrzebom organizacyjnym Zamawiającego.	Wykonawca uzgadnia harmonogram i agendę warsztatów z przedstawicielem Zamawiającego przed realizacją.

5.6. Autoryzowane szkolenie Fortigate Administrator

Zakres	Opis
Nazwa szkolenia	Szkolenie z podstaw administracji FortiGate prowadzone przez ośrodek posiadający autoryzację Fortinet dla prowadzenia szkoleń oraz wydawania certyfikatów potwierdzających kompetencje.
Kod szkolenia	FT-FGT-ADM
Forma szkolenia	Distance learning (zdalnie z trenerem)
Materiały szkoleniowe	W postaci elektronicznej, podręczniki zgodnie z agendą i zakresem producenta firmy Fortinet

Zakres	Opis
Termin szkolenia	Uzgodniony z Zamawiającym jednak nie dłuższy niż 30.04.2026
Voucher egzaminacyjny	Tak – ważny co najmniej 6 miesięcy od chwili ukończenia szkolenia
Zakres szkolenia	<p>Uczestnicy nauczą się:</p> <ul style="list-style-type: none"> • Podstaw działania zapory sieciowej FortiGate • Uwierzytelniania użytkowników • Konfiguracji wysokiej dostępności (HA) • Tworzenia tuneli SSL VPN i IPsec VPN (site-to-site) • Wdrażania Fortinet Security Fabric • Stosowania profili bezpieczeństwa: IPS, antywirus, filtrowanie stron, kontrola aplikacji
Cele szkolenia	<p>Po ukończeniu szkolenia uczestnik będzie potrafił:</p> <ul style="list-style-type: none"> • Skonfigurować podstawowe ustawienia sieciowe FortiGate • Kontrolować dostęp administratora • Używać GUI i CLI do administracji • Tworzyć reguły zapory i NAT • Analizować i konfigurować routing • Uwierzytelniać użytkowników i monitorować ich aktywność • Wdrażać FSSO z AD • Kontrolować ruch SSL/TLS • Konfigurować profile bezpieczeństwa • Stosować kontrolę aplikacji • Tworzyć VPN SSL i IPsec • Konfigurować SD-WAN • Wdrażać HA • Diagnozować i rozwiązywać problemy

Zakres	Opis
Grupa docelowa	Osoby odpowiedzialne za administrację i bezpieczeństwo sieci, w szczególności administratorzy IT, inżynierowie bezpieczeństwa, specjaliści ds. sieci

6. **Zamówienie jest przeznaczone do użytku osób fizycznych, zatem Zamawiający uwzględnił w opisie przedmiotu zamówienia wymagania w zakresie dostępności osób z niepełnosprawnością**

