Załącznik nr 1
do Zapytania Ofertowego

Opis Przedmiotu Zamówienia

1. Słownik terminów

Termin / skrót	Opis
Zgłoszenie zarejestrowane przez Zamawiającego w systemie SOI	Zarejestrowanie zgłoszenie w systemie w kategorii: - awaria - konsultacja Awaria to brak możliwości korzystania z usługi przez Użytkowników Systemu z punktu widzenia celów biznesowych. Awaria może być sklasyfikowana jako: • Błąd Krytyczny, • Błąd Poważny, • Usterka. Konsultacja - Udzielanie konsultacji przez Wykonawcę polega na zapewnieniu stałej opieki konsultantów, których zadaniem jest pomoc przy rozwiązywaniu bieżących zagadnień związanych z eksploatacją systemu które nie mogą być skategoryzowane jako awaria.
Błąd Krytyczny	Niepoprawne działanie usługi uniemożliwiające realizację zadań określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu w zakresie zapewnienia prawidłowego funkcjonowania Systemu, w tym w szczególności brak działania Systemu, zagrożenie dla bezpieczeństwa Systemu lub błędne składowanie danych w bazie Systemu.
Błąd Poważny	Niepoprawne działanie usługi utrudniające realizację zadań określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu w zakresie zapewnienia prawidłowego funkcjonowania Systemu.
Usterka	Każdy inny Błąd nie będącym Błędem Krytycznym Lub Poważnym czyli niepoprawne działanie usługi lub niezgodność funkcjonalności Systemu z warunkami określonymi w Dokumentacji Systemu.
Czas Naprawy	Czas między zgłoszeniem Awarii, a jej skutecznym i trwałym usunięciem, zgłoszonym przez Wykonawcę.
Czas Reakcji	Czas między zgłoszeniem Awarii, a uzyskaniem potwierdzenia przystąpienia do jego usunięcia.
Dni Robocze	Każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.
Dokumentacja	Wszelka dokumentacja wytworzona przez Wykonawcę w ramach dostarczenia usługi, dotycząca aspektów technicznych, funkcjonalnych i użytkowych związanych z korzystaniem z Systemów Zamawiającego.
FAZ VM	Forti Analyzer Virtual Machine
Godziny Robocze	Godziny od 8:00 do 16:00 w Dni Robocze.
Infrastruktura Chmury Obliczeniowej	Infrastruktura znajdująca się w dyspozycji Dostawcy Chmury, umożliwiająca dostarczanie przez niego Usług Chmury Obliczeniowej. Infrastruktura znajduje się w minimum dwóch lokalizacjach i z punktu widzenia architektury jest rozproszonym geograficznie klastrem niezawodnościowym HA.
Infrastruktura MRiT	Wydzielona infrastruktura zlokalizowana w siedzibie Zamawiającego dedykowana dla: Systemu CEIDG (TEST), Hurtowni Danych (TEST) i Biznes.gov.pl (TEST i PROD) - Punktu Informacyjnego dla Przedsiębiorcy oraz systemów pomocniczych (m.in.. backup, monitoring, ITSM) .
Lokalizacja	Określenie fizycznego miejsca, w którym są eksploatowane Instancje Hurtowni. Z punktu widzenia Umowy istnieją dwie lokalizacje: • Lokalizacja Chmura, • Lokalizacja MRiT
Lokalizacja Chmura	Zarządzana przez Dostawcę Chmury wirtualna platforma widoczna przez Wykonawcę jako zestaw usług typu IaaS i Pass. Z technicznego punktu widzenia jest to klaster HA rozproszony geograficznie (dwie fizyczne lokalizacje) pracujący w trybie "active –active"
Lokalizacja MRiT	Lokalizacja centrum przetwarzania danych mieszczące się w siedzibie

	Zamawiającego, dedykowane na potrzeby funkcjonowania CEIDG, Hurtowni danych i Biznes.gov.pl.
Zamawiający (MRiT)	Ministerstwo Rozwoju i Technologii
Naprawa Awarii	Trwałe usunięcie Awarii poprzez usunięcie przyczyn powstania Awarii skutkujące przywróceniem pełnej sprawności usługi, w tym również zakończenie innych działań naprawczych.
Obejście Awarii	Wykonanie tymczasowego sposobu korzystania z innych funkcji lub komponentów usługi, pozwalającego na realizację zadań Zamawiającego określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu, których normalna realizacja jest utrudniona lub uniemożliwiona z powodu wystąpienia Awarii; zastosowane rozwiązanie nie może powodować utraty lub zmniejszenia funkcjonalności Systemu.
Okno Dostępności	Czas w ciągu doby poza Oknem Serwisowym. Zamawiający wymaga aby w czasie Okna Dostępności systemy objęte Usługą były w pełni funkcjonalne i dostępne.
Okno Serwisowe	Czas niedostępności całego systemu lub jego określonych funkcji uzgodniony pomiędzy Zamawiającym a Wykonawcą, przeznaczony na wykonywanie wszelkich niezbędnych prac serwisowych, przeglądów, aktualizacji oprogramowania oraz wgrywania nowych wersji oprogramowania. Okna serwisowe mogą mieć miejsce poza Godzinami Roboczymi.
SLA (Service Level Agreement)	Poziom dostępności świadczonych usług wyrażony w % w skali okresu rozliczeniowego.
System	System CEIDG wraz z hurtownią danych i System Biznes.gov.pl.
Umowa	Umowa zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi aneksami i załącznikami do Umowy.
Ustawa	Ustawa z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy
Użytkownik	Osoba korzystająca z Systemu lub jego poszczególnych części.
Zgłoszenie	Przekazanie Wykonawcy zawiadomienia o Awarii lub konsultacji.
WAF	Web Application Firewall
SNI	Server Name Identification
System Obsługi Eksploatacji	System składający się z dwóch systemów: • Systemu Obsługi Incydentów (SOI) • Systemu Obsługi Zleceń
Mitygacja	Działania, które mają na celu ograniczanie ryzyka i skutków ataków na usługi Zamawiającego.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usług utrzymania wdrożonej u Zamawiającego kompleksowej usługi ochrony klasy Web Application Firewall (WAF) dla Systemów Zamawiającego, dostępnych publicznie z sieci Internet.
System WAF wyposażony jest w zaawansowane mechanizmy detekcji i reakcji na ataki, między innymi takie jak SQL Injection, Cross-Site Scripting (XSS), fałszowanie żądań międzywitrynowych (CSRF) oraz inne techniki stosowane przez cyberprzestępców.

Ochronie podlega 16 aplikacji webowych oraz usługi 2 serwerów DNS Autorytatywnych z analizą bezpieczeństwa w dostarczonych rozwiązaniach.

Rozwiązanie oparte jest na technologii firmy Akamai, obejmujące następujące komponenty:

1) App & API Protector with Delivery;

2) Application Load Balancing;

3) API Gateway;

4) Edge DNS;

5) Managed Security Services 3.0, w tym zawarty Security Operations Center (SOC) aktywny, w skrócie SOC aktywny;

6) Integrating Akamai Products;

W ramach realizacji zamówienia Wykonawca zapewni odnowienie subskrypcji na okres zgodny z wariantem realizacji zamówienia, tj. 2 miesiące, obejmujący co najmniej:

- Akamai App & API Protector with delivery,
- Akamai Application Load Balancing,
- Akamai API Gateway,
- Akamai Edge DNS,
- Akamai Managed Security Services (MSS),

Dostawa odnowienia subskrypcji musi nastąpić w terminie do 5 dni od dnia podpisania umowy, lecz nie później niż do **13.09.2026 r.**

3. Termin realizacji

2 miesiące od dnia podpisania umowy

Rozpoczęcie świadczenia usługi musi nastąpić w terminie **od 13.09.2026 r.**

4. Zakres usługi

W ramach świadczenia usługi utrzymania Wykonawca zobowiązany jest do zapewnienia, aby system ochrony przez cały okres obowiązywania umowy nieprzerwanie spełniał następujące wymagania:

4.1 Zaawansowane Funkcje Ochrony

Numer wymagania	Opis wymagania
WT 1	System Web Application Firewall musi oferować zaawansowaną ochronę przed najnowszymi i najbardziej rozpowszechnionymi zagrożeniami internetowymi, w tym, ale nie ograniczając się do, ataków typu SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), oraz ataków typu Denial-of-Service (DoS/DdoS).
WT 1.1	Ochronie podlegają aplikacje wytworzone dla Ministerstwa Rozwoju i Technologii oparte o zróżnicowany stos technologiczny. Wymaganie jest dostosowanie reguł bezpieczeństwa we współpracy z zespołem technicznym Zamawiającego oraz podmiotami odpowiedzialnymi za utrzymanie i rozwój chronionych aplikacji.
WT 1.2	Połączenie systemu ochrony z chronionymi aplikacjami terminowane będzie za pomocą protokołu HTTPS.
WT 1.3	Dla każdej z chronionych aplikacji konieczna jest implementacja zestawu reguł „OWASP Core Rule Set v3". W przypadku udostępnienia zaktualizowanego zbioru, konieczne będzie wykonanie modyfikacji reguł w celu spełnienia wymagań nowej wersji. Dopuszczalne jest zastosowanie alternatywnego zbioru reguł np. dostarczany przez producenta rozwiązania. Musi on jednak zapewniać poziom ochrony nie gorszy niż wyżej wymieniony.
WT 1.4	Dla każdej z chronionych aplikacji konieczne jest wykonanie dogłębnej analizy i wprowadzenie reguł dedykowanych dla danej aplikacji.
WT 1.5	System musi wykorzystywać zaawansowane algorytmy i mechanizmy uczenia maszynowego do automatycznego wykrywania i prewencyjnego blokowania nowych i złożonych ataków, nawet tych niezdefiniowanych wcześniej w bazach danych zagrożeń.

WT 1.6	System musi mieć zaimplementowane zintegrowane mechanizmy ochrony, które pozwalają na szybkie reagowanie na ataki typu zero-day, czyli ataki wykorzystujące nieznane wcześniej luki bezpieczeństwa.
WT 1.7	System musi mieć możliwość blokowania lub ograniczania dostępu na podstawie geolokalizacji lub wyspecyfikowanej listy adresów IP, umożliwiająca prewencyjne odcięcie potencjalnych zagrożeń z określonych regionów lub adresów. Funkcjonalność musi umożliwiać konfigurację zabezpieczenia na określony czas zarówno dla pojedynczego adresu IP oraz z degradacją do konkretnej usługi podlegającej ochronie. Po upłynięciu określonego czasu adres powinien być usuwany z listy. Musi istnieć możliwość odblokowania zablokowanego zbioru adresów na zlecenie Zamawiającego. System musi umożliwiać zdefiniowanie tzw. „białej listy", czyli puli adresów lub lokalizacji geograficznych, które w przypadku wystąpienia naruszeń nie będą blokowane. System musi umożliwiać definicję wielu takich list dostępowych np. dedykowanej dla każdej z aplikacji.
WT 1.8	System musi posiadać tzw. „Virtual Patching" czyli funkcjonalność pozwalającą na szybkie zabezpieczanie znanych luk w zabezpieczeniach, nawet zanim zostanie wydany oficjalny patch przez producenta oprogramowania.
WT 1.9	System musi umożliwiać ochronę przed automatycznymi skryptami (botami), które mogą prowadzić do scrapingu danych, ataków brute-force, czy fałszywego ruchu na stronie.
WT 1.10	System musi być wyposażony w specjalistyczne rozwiązania do ochrony interfejsów API oraz serwisów webowych, które są często narażone na specyficzne rodzaje ataków. W tym minimum odkrywać i powstrzymywać ataki oparte na logice biznesowej zarówno dla aplikacji internetowych, jak i punktów końcowych API, wykorzystując uczenie maszynowe i sztuczną inteligencję. Przeprowadzać zautomatyzowane wykrywanie ruchu API, w tym - Wykorzystywane aktywne punkty końcowe - Statystyki kodów odpowiedzi Możliwość egzekwowania pozytywnego modelu bezpieczeństwa w oparciu o schemat obejmujący powyższe parametry w oparciu zarówno o zautomatyzowane wyniki wykrywania, jak i niestandardowy, ręcznie przesłany schemat Open API v3, w tym egzekwowanie sekwencji i zawartość ścieżki, zapytania, nagłówka, plików cookie, treści i innych parametrów. Obsługa i wymuszanie wzajemnego uwierzytelniania TLS, w tym dla urządzeń klienckich iOS i IOT, z opcją przesyłania wielu niestandardowych certyfikatów urzędów certyfikacji. Ochrona przed złośliwymi zapytaniami do interfejsów API GraphQL Weryfikacja i wydawanie tokenów JWT, kluczy API i Oauth 2.0 przekazywanych do interfejsów API w celu zapobiegania manipulacjom i atakom typu replay.
WT 1.11	System musi oferować możliwość automatycznej kategoryzacji wykrywanych incydentów minimum na poziomach krytycznym, poważnym, średnim i umiarkowanym. Zamawiający dopuszcza użycie innych nazw dla kategorii z zachowaniem minimum czteropoziomowej skali kategoryzacji.
WT 1.12	Jako dodatkowy komponent systemu dostarczona zostanie usługa Autorytatywnego DNS.
WT 1.13	Serwery DNS powinny być odseparowane od siebie geograficznie oraz być udostępnione z różnych podsieci adresów publicznych.
WT 1.14	Serwery DNS powinny być udostępnione z łącz objętych ochroną AntyDDoS
WT 1.15	Wszystkie komponenty systemu wykorzystane do budowy muszą spełniać kryteria rozwiązań klasy enterprise. Wszystkie komponenty systemu powinny być objęte aktualnym wsparciem producenta oraz aktualnymi kontraktami serwisowymi.

4.2. Wykrywanie i Reagowanie w Czasie Rzeczywistym

Numer wymagania	Opis wymagania
WT 2	Rozwiązanie musi zapewniać zdolność do wykrywania i blokowania ataków w czasie

	rzeczywistym, z minimalnym wpływem na wydajność aplikacji internetowych.
WT 2.1	System ochrony musi spełniać warunki dostępności na poziomie SLA 99,9% liczone w cyklu miesięcznym tj. 43 minut 28 sekund niedostępności w każdym miesiącu rozliczeniowym.
WT 2.2	Zamawiający wymaga, aby wykonawca prowadził monitoring pod kątem dostępności dostarczonego rozwiązania w trybie ciągłym i będzie reagował na incydenty. W ramach reakcji na incydent Zamawiający wymaga, aby wykonawca monitorował logi zdarzeń i alerty generowane przez system oraz wykonywał modyfikację reguł na dostarczonym systemie w celu uniemożliwienia wykorzystania podatności mogącej prowadzić do incydentu bezpieczeństwa.
WT 2.3	Rozliczanie dostępności będzie oparte o zewnętrzny system monitoringu dostarczony przez Zamawiającego, który wykonuje testy w trybie ciągłym poprzez wykonywanie zdefiniowanych scenariuszy np. logowanie do systemu Zamawiającego. Testy wykonywane są z minimum 3 lokalizacji rozdzielonych geograficznie, a incydent jest generowany automatycznie na podstawie stwierdzenia błędu dla większości stacji monitorowania. Na życzenie wykonawcy Zamawiający udostępni podgląd do konfiguracji systemu lub powiadomień generowanych przez zewnętrzny system monitoringu. Za naruszenie będzie uznawana niedostępność spowodowana przez dowolny z elementów dostarczonych w ramach systemu ochrony.
WT 2.4	Do czasu niedostępności nie będą wliczane wcześniej ustalone przerwy serwisowe. Informacja o przerwie serwisowej musi zostać ustalona i zaakceptowana przez Zamawiającego nie później niż 24 godziny przed jej wykonaniem. Sumaryczny czas trwania przerw serwisowych nie może przekroczyć 4 godzin w ujęciu miesięcznym. Przerwy serwisowe powinny być planowane i prowadzone w godzinach 22:00-4:00 każdego dnia miesiąca. Na czas przerw serwisowych Wykonawca będzie udostępniał informację dla internautów o przerwie serwisowej. Treść komunikatów dostarczać będzie Zamawiający.
WT 2.5	Zamawiający wymaga, aby w przypadku wykrycia ataku przez WAF, Wykonawca dokonał natychmiast wstępnej analizy i wdrożył konieczne zabezpieczenia. Wykonawca musi wykonywać przegląd zdarzeń i alertów na urządzeniu nie rzadziej niż co 24 godziny w przypadku wystąpień o kategorii krytycznej, wysokiej lub średniej dla których nie wystąpiła akcja prevent.
WT 2.6	Wykonawca ma prawo wymagać przeprowadzenia testów działania rozwiązania WAF przez Zamawiającego lub podmioty utrzymujące poszczególne elementy chronione. W przypadku pozytywnego potwierdzenia wykonaniu testów, jeżeli zmiany bezpośrednio spowodują niedostępność, to nie będzie ona odliczana od parametrów SLA.

4.3. Integracja z Istniejącymi Systemami

Numer wymagania	Opis wymagania
WT 3	Rozwiązanie powinno być kompatybilne i zintegrowane z istniejącymi systemami Zmawiającego. Zamawiający nie dopuszcza ingerencji w kod źródłowy aplikacji oraz w infrastrukturę Zamawiającego.
WT 3. 1	Zamawiający wymaga, aby wykonawca udostępnił logi zdarzeń generowanych w ramach działania systemu. Dane będą przesyłane do systemu klasy SIEM oraz Log Management dostarczonych przez Zamawiającego. Wykonawca systemu wesprze Zamawiającego przy integracji z wyżej wymienionymi systemami w zakresie udostępnienia danych. Integracja będzie zrealizowana z użyciem powszechnych protokołów wymiany tego typu danych np. rsyslog, pliki płaskie.
WT 3.2	Konieczne może być udostępnienie usługi maszyny wirtualnej lub appliance dostarczonego przez producenta systemu SIEM lub Log Management. Udostępniony w ten sposób zasób pełnił będzie rolę tzw. „Kolektora logów”, którego celem będzie oczyszczanie i buforowanie wysyłanych danych do systemu klasy SIEM oraz Log Management dostarczonych przez Zamawiającego. Jego istnienie jest zależne od

	konieczności oszczędności pasma, filtrowania zbędnych informacji lub zapewnienia odpowiedniego zabezpieczenia warstwy transportowej.
WT 3.3	Wykonawca będzie odpowiedzialny za utrzymanie dostarczonej warstwy infrastruktury. Wymagany jest ciągły monitoring usługi w sposób automatyczny. Zamawiający wymaga, aby w przypadku stwierdzenia nieprawidłowości wysłane zostało powiadomienie na kanały wspólnie uzgodnione z Zamawiającym np. adres e-mail.
WT 3.4	Pasmo przesyłowe wykorzystane do przekazywania dzienników zdarzeń, nie może zostać odliczone od gwarantowanej przepustowości w ramach usługi ochrony danych przeznaczonej dla ruchu użytkowników chronionych aplikacji.
WT 3.5	Zamawiający wymaga, aby dostarczona usługa Autorytatywnego DNS znajdowała się w minimum dwóch niezależnych ośrodkach przetwarzania. Usługa musi znajdować się za ochroną DdoS opisaną w wymaganiach w WT 4.
WT 3.6	Zamawiający wymaga, aby dostarczona usługa posiadała automatyczne wykrycie end pointów API przy niskim nakładzie pracy ze strony Zamawiającego.

4.4. Skalowalność i Elastyczność

Numer wymagania	Opis wymagania
WT 4	System musi wykazywać wysoką skalowalność, aby móc dostosować się do rosnących potrzeb Zamawiającego, wraz ze wzrostem ruchu sieciowego oraz ewolucją struktury IT. Dla przyjętych parametrów należy przyjąć założenie wzrostu zapotrzebowania o 10% rok do roku.
WT 4.1	Usługa ochrony musi być udostępniona za usługą AntyDDoS.
WT 4.2	Zamawiający wymaga, aby dostarczony system był chroniony przed atakami DdoS. Wymaga się aby punkt styku z publiczną siecią Internet był chroniony przed atakami wolumetrycznymi o minimalnej pojemności 40 Gbps i 10 Mpps za pomocą dedykowanej infrastruktury lub usługi mitygacji tego typu ataków.
WT 4.3	Mitygacja ataków DdoS i związane z tym niedostępności, będą liczone jako niedostępność usługi. Akceptowalne jest odliczenie czasu koniecznego na uruchomienie procedur automatycznych związanych z mitygacją tego typu ataków jednak nie może być on dłuższy niż 10 minut, a warunkiem nie uwzględnienia tego czasu jako niedostępności w rozliczeniu SLA jest przekazanie przez Wykonawcę odpowiedniego raportu poświadczającego wystąpienie ataku klasy DdoS. Łączny czas odliczenia nie może być dłuższy niż 30 minut w skali jednego miesiąca rozliczeniowego.
WT 4.4	System musi korzystać z co najmniej z dwóch niezależnych połączeń internetowych dostarczanych przez różnych dostawców.
WT 4.5	W przypadku awarii jednego z łącz, system automatycznie i bez przestoju musi przełączyć ruch na aktywne, sprawne łącze.
WT 4.6	System musi umożliwiać implementację przełączania ruchu użytkowników między środowiskami podstawowym i zapasowym zlokalizowanym w centrach przetwarzania danych Zamawiającego. Implementacja rozwiązania musi pozwalać na skonfigurowanie mechanizmu weryfikacji działania ang. Health-Check przy użyciu żądań http lub HTTPS i oparcia o niego automatycznej decyzji o przełączeniu ruchu na środowisko zapasowe
WT 4.7	System musi umożliwiać implementację przełączania ruchu użytkowników między środowiskami podstawowymi i zapasowymi zlokalizowanymi w centrach przetwarzania danych Zamawiającego. Funkcjonalność przełączenia powinna być dostępna dla Zamawiającego. Czas realizacji przełączenia nie może być dłuższy niż 60 minut. Nie wliczając w to propagacji rekordów DNS.
WT 4.8	System musi obsługiwać funkcjonalność server-side SNI (Server Name Identification).

4.5. Zarządzanie Konfiguracją i Politykami Bezpieczeństwa

Numer	Opis wymagania

wymagania	
WT 5	Rozwiązanie musi umożliwiać łatwe zarządzanie konfiguracją oraz dostosowywanie polityk bezpieczeństwa, aby sprostać specyficznym wymaganiom i regulacjom prawnym.
WT 5.1	Na zlecenie Zamawiającego wykonawca udostępni pełną konfigurację systemu w zakresie działających reguł bezpieczeństwa w postaci pliku konfiguracyjnego lub listy reguł wraz z szczegółami konfiguracyjnymi, pozwalające na przeprowadzenie eksperckiej analizy w ramach audytów bezpieczeństwa prowadzonych w imieniu Zamawiającego przez wyspecjalizowane w tych zadaniach podmioty.
WT 5.2	Zamawiający zastrzega sobie prawo wykonywania testów bezpieczeństwa i działania dostarczonego systemu przez wyspecjalizowane zespoły w zakresie testów wydajności i bezpieczeństwa cyfrowego. Zamawiający zobowiązuje się do poinformowania wykonawcy o zamiarze przeprowadzenia testów, terminie jego wykonania oraz jego zakresie. Informacja musi być przekazania nie później niż 2 dni robocze przed planowanym wykonaniem prac.
WT 5.3	Zamawiający wymaga, aby rozwiązanie umożliwiało przeprowadzenie testów funkcjonalnych wprowadzonych zmian w konfiguracji usługi ochrony. Wymagana jest dodatkowa warstwa testowa konfiguracyjnie tożsama z środowiskiem produkcyjnym. Warstwa testowa nie musi gwarantować pełnej przepustowości produkcyjnego systemu. System ma pozwalać na wykonanie testów funkcjonalnych aplikacji. Dostęp do warstwy testowej musi być możliwy poprzez modyfikację pliku hosts na stacji testowej lub poprzez modyfikację rekordu w wewnętrznym serwerze DNS. Dostarczone środowisko testowe może być wydzieloną logicznie częścią środowiska produkcyjnego. Środowisko testowe nie podlega rygorom parametrów SLA.
WT 5.4	Zamawiający wymaga aby, wszystkie opcje konfiguracyjne dostępne w GUI powinny być obsługiwane poprzez interfejs API. Funkcje eksperymentalne i beta powinny być dostępne za pośrednictwem interfejsu API, nawet jeśli nie są dostępne w interfejsie GUI. Producent powinien dostarczyć i wspierać pakiet Terraform

4.6. Raportowanie i Analiza

Numer wymagania	Opis wymagania
WT 6	System musi oferować zaawansowane funkcje raportowania i analizy, umożliwiające dogłębną ocenę stanu bezpieczeństwa oraz identyfikację potencjalnych słabych punktów.
WT 6.1	System musi oferować możliwość szczegółowego rejestrowania wszystkich zdarzeń związanych z bezpieczeństwem, w tym prób ataków, naruszeń polityk bezpieczeństwa, błędów konfiguracyjnych i anomalii w ruchu sieciowym.
WT 6.2	Funkcja analizy musi umożliwiać identyfikację i śledzenie trendów oraz wzorców w zakresie ataków i zagrożeń, co pozwala na wczesne wykrywanie potencjalnych słabych punktów i luk w zabezpieczeniach.
WT 6.3	System musi umożliwiać generowanie spersonalizowanych raportów, dostosowanych do różnych poziomów użytkowników, od technicznych operatorów bezpieczeństwa po kierownictwo. Dostarczenie raportów powinno być możliwe automatycznie na adres e-mail, udział sieciowy lub link do pobrania. Moduł raportowy musi umożliwiać przekazanie danych analitycznych w formie pliku pdf, csv jak i surowych plików logów w formacie przeznaczonym do odczytu maszynowego.
WT 6.4	Mechanizm powiadomień w czasie rzeczywistym musi informować odpowiednie osoby lub zespoły o krytycznych zdarzeniach bezpieczeństwa, umożliwiając szybką reakcję.
WT 6.5	System musi oferować interaktywne narzędzia do wizualizacji danych, które ułatwiają zrozumienie złożonych danych związanych z bezpieczeństwem i pomagają w ich analizie.
WT 6.6	System musi oferować funkcje audytu i przeglądu historii zdarzeń, umożliwiające śledzenie zmian, dostępów i operacji przeprowadzanych w systemie. W szczególności w zakresie zmian w konfiguracji.

WT 6.7	System musi dać możliwość dostępu do raportów i analiz za pomocą przeglądarki internetowej
WT 6.8	System musi udostępniać funkcjonalność monitorowania ruchu webowego tj. wolumen obsługiwanego ruchu w rozdziale na konkretne chronione aplikacje jak i sumarycznie. Udostępniać informację o użytkownikach tj. adres IP, pochodzenie geograficzne, system operacyjny, przeglądarka. Udostępniać informację o typach ataków, ich pochodzenie, akcję jaka została podjęta,.
WT 6.9	System musi umożliwiać przegląd danych do 90 dni wstecz.
WT 6.10	System musi umożliwiać prezentację danych w postaci konfigurowalnego dashboardu.
WT 6.11	System musi umożliwiać prezentację listy aktualnie nałożonych blokad.
WT 6.12	Wszystkie komponenty i możliwości rozwiązania powinny być dostarczane jako pojedyncza platforma SaaS oparta na chmurze, bez potrzeby dodatkowej integracji między komponentami, pulpitami nawigacyjnymi do analizy i śledzeniem żądań pakietów poza pojedynczą ścieżką pakietu

4.7. Wsparcie rozwiązania

Numer wymagania	Opis wymagania
WT 7	Zamawiający wymaga, aby dostawca zapewnił pełne wsparcie techniczne i serwisowe, w tym reakcję na zgłoszenia zgodną z warunkami SLA, regularne aktualizacje oprogramowania oraz doradztwo w zakresie najlepszych praktyk bezpieczeństwa w ramach dostarczonego rozwiązania.
WT 7.1	Dostawca musi zapewnić dedykowany zespół wsparcia, który będzie dostępny 24/7 do reagowania na zgłoszenia i rozwiązywania problemów. Zespół ten musi posiadać wysokie kwalifikacje i doświadczenie w zakresie cyberbezpieczeństwa oraz zarządzania systemami WAF.
WT 7.2	Dostawca musi przeprowadzać regularne aktualizacje oprogramowania, w tym łatki bezpieczeństwa, aby system był zawsze zabezpieczony przed najnowszymi zagrożeniami.
WT 7.3	Dostawca musi zapewnić wsparcie w zarządzaniu incydentami bezpieczeństwa, w tym wsparcie w analizie przyczyn i rekomendowanie działań naprawczych.
WT 7.4	W przypadku stwierdzenia incydentu bezpieczeństwa Zamawiający wymaga, aby Wykonawca przeprowadził pełną analizę bezpieczeństwa w zarządzanym przez siebie obszarze, wynikiem czego musi być raport zawierający pełną analizę oraz argumentację potwierdzoną dowodami.
WT 7.5	Dla każdego zidentyfikowanego zagrożenia musi zostać przeprowadzona analiza wpływu na bezpieczeństwo danych osobowych ze szczególnym uwzględnieniem prawdopodobieństwa wycieku danych (ang. data breach).
WT 7.6	W przypadku potwierdzenia wycieku danych Wykonawca we współpracy z Zamawiającym ma obowiązek przeprowadzenia analizy śledczej, której celem jest ocena skutków naruszenia.
WT 7.7	Analiza zdarzenia i realizacja czynności w zakresie incydentów bezpieczeństwa mającego musi być przeprowadzona przez Wykonawcę bez ponoszenia dodatkowych kosztów przez Zamawiającego. Wszystkie czynności muszą być zakończone raportem, a jego zakres musi obejmować wszystkie elementy dostarczone przez Wykonawcę w ramach zamówienia.
WT 7.8	Zamawiający wymaga, aby w ramach rozliczenia miesięcznego Wykonawca wykonywał zbiorczy raport zawierający informację w zakresie wykrytych zdarzeń, podjętych akcji, zmian w konfiguracji, dostępności systemu oraz rekomendacji dotyczących systemu. Ostateczny szablon raportu zostanie ustalony po podpisaniu umowy.

4.8. Zgodność z Standardami Bezpieczeństwa

Numer	Opis wymagania

wymagania	
WT 8	Rozwiązanie musi być zgodne z międzynarodowymi standardami i praktykami bezpieczeństwa oraz spełniać lokalne przepisy dotyczące ochrony danych.
WT 8.1	Rozwiązanie musi być zaprojektowane zgodnie z zaleceniami Open Web Application Security Project (OWASP) Top 10, obejmującymi najważniejsze zagrożenia dla aplikacji internetowych, w tym zapobieganie atakom takim jak iniekcje SQL, Cross Site Scripting (XSS), i innym powszechnym lukom w zabezpieczeniach.
WT 8.2	Dostawca musi posiadać certyfikat ISO/IEC 27001 lub SOC2, na potwierdzenie, że jego system zarządzania bezpieczeństwem informacji i wewnętrzne procedury spełniają międzynarodowe standardy w zakresie bezpieczeństwa informacji.
WT 8.3	System musi spełniać wymagania Ogólnego Rozporządzenia o Ochronie Danych (GDPR) oraz innych lokalnych przepisów dotyczących ochrony danych, co obejmuje zarządzanie danymi osobowymi i ich bezpieczeństwem.
WT 8.4	Zastosowanie ram bezpieczeństwa cybernetycznego opracowanych przez National Institute of Standards and Technology (NIST), które obejmują identyfikację, ochronę, wykrywanie, reagowanie i odzyskiwanie w kontekście zagrożeń cybernetycznych.
WT 8.5	Rozwinięcie i utrzymanie szczegółowych polityk bezpieczeństwa oraz procedur, które są w pełni zgodne z wyżej wymienionymi standardami i najlepszymi praktykami. Zamawiający wymaga, aby wykonawca dostarczył dokumenty potwierdzające wdrożenia powyższych standardów w postaci certyfikatów i opisów obowiązujących procedur.
WT 8.6	Wykonawca w przypadku wykrycia incydentów w środowisku Zamawiającego będzie stosował się do polityk Systemu Zarządzania Bezpieczeństwem Informacji obowiązujących u Zamawiającego (do wglądu w siedzibie).

4.9. Parametry ilościowe i pojemnościowe

Numer wymagania	Opis wymagania
WT 10	Każdy obiekt ochrony musi posiadać swój dedykowany adres usługi (np. publiczny adres IP, rekord CNAME), który zostanie skierowany ruch z serwerów DNS Zamawiającego.
WT 10.1	Łącze obsługujące ochronę obiektów musi gwarantować przepustowość na poziomie 600Mbps.
WT 10.2	W ramach ochrony muszą zostać dostarczone dwa serwery DNS Autorytatywne. Zamawiający posiada w swojej infrastrukturze serwer master, z którego publikowane będą konfiguracje dla serwerów udostępnionych w ramach usługi.
WT 10.3	Szacowany przepływ ruchu w ramach chronionych aplikacji to 20TB miesięcznie.
WT 10.4	Szacunkowa ilość żądań http do obsługi to 39 milionów miesięcznie w tym 1,2 miliona do chronionych usług API.

5. Wymagania dotyczące usuwania Awarii (WA)

Numer wymagania	Opis wymagania
WA 1	Zgłoszenia Awarii będą dokonywane za pośrednictwem SOI przez upoważnionych pracowników Wykonawcy oraz Zamawiającego. Zamawiający zobowiązany jest przekazać Wykonawcy w terminie 1 tygodnia od dnia zawarcia Umowy listę upoważnionych pracowników Zamawiającego. Zmiana osób wskazanych w ww. liście następuje poprzez pisemne powiadomienie Wykonawcy bez konieczności podpisywania aneksu do Umowy.
WA 2	Jeżeli Awaria została wykryta przez pracowników Wykonawcy lub Wykonawca otrzymał informację o wystąpieniu Awarii z dowolnego zewnętrznego źródła, obowiązkiem Wykonawcy jest niezwłocznie przystąpienie do usuwania Awarii oraz poinformowanie Zamawiającego o wystąpieniu Awarii oraz zarejestrowanie Awarii w SOI w czasie nie dłuższym niż 0,5 godziny.
WA 3	Przyjmuje się, że Zgłoszenie Usunięcia Awarii rozpoczyna się z chwilą

	zarejestrowania Awarii w SOI.
WA 4	Zamawiający ma prawo do zgłaszania Awarii przez cały rok, 7 dni w tygodniu, 24 godziny na dobę. Czas na usunięcie Awarii rozpoczyna się w momencie Zgłoszenia Usunięcia Awarii.
WA 5	Jeśli dla dokonania usunięcia Awarii obiektywnie niezbędne będzie podjęcie przez Zamawiającego określonych czynności lub przekazanie dodatkowych wyjaśnień Wykonawca może się zwrócić do Zamawiającego o nie jeden raz. Czas na udzielanie wyjaśnień nie będzie wliczany do czasu obsługi Zgłoszenia Usunięcia Awarii. Przy obsłudze złożonych Awarii Zamawiający może zdecydować o wielokrotnym zadawaniu pytań i udzielaniu odpowiedzi przez Zamawiającego.
WA 6	Informację o usunięciu Awarii Wykonawca będzie zgłaszał w Systemie Obsługi Incydentów.
WA 7	O zakończeniu usunięcia Awarii decyduje Zamawiający.
WA 8	Skuteczne usunięcie Awarii Zamawiający będzie potwierdzał w Systemie Obsługi Incydentów.
WA 9	Jeżeli Wykonawca nie dokona naprawy w terminach, wskazanych w Tabeli 1 umieszczonej poniżej, Zamawiający może: a) obciążyć Wykonawcę karą umowną na zasadach opisanych w Umowie, b) zawiadamiając uprzednio Wykonawcę, usunąć Awarię we własnym zakresie lub powierzyć jej usunięcie innemu podmiotowi trzeciemu na koszt Wykonawcy. Naprawa nie powoduje wygaśnięcia oraz utraty jakichkolwiek praw wynikających z tytułu gwarancji.

Tabela 1 Wartości Czasów Naprawy (od czasu Rejestracji Zgłoszenia)

Lp.	Parametr	Błąd Krytyczny (godziny)	Błąd Poważny (godziny)	Usterka (godziny)
1	Czas Reakcji	0,5	0,5	0,5
2	Czas zastosowania Obejścia	0,5	1	nie dotyczy
3	Czas Naprawy	4	8	24