

OPIS PRZEDMIOTU ZAMÓWIENIA

I. 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.

Przedmiot zamówienia dotyczy usług wymienionych w niniejszym OPZ, w ilościach zgodnych z poniższym wykazem lub równoważne zgodnie z warunkami określonymi w rozdziale III.

L.p.	Numer katalogowy	Produkt	Liczba produktów	Okres świadczenia usług
1	M-LC-169584	App & API Protector with delivery	1	4 miesiące
2	M-LC-160433	Application Load Balancing	1	4 miesiące
3	M-LC-161591	API Gateway	1	4 miesiące
4	M-LC-62373	Edge DNS	1	4 miesiące

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie 4 miesięcy od dnia 1 października 2026 r.

III. AKTUALNY STAN

Zamawiający posiada wdrożone usługi ochrony publicznie dostępnych aplikacji webowych klasy Web Application Firewall (WAF), w zakresie wymienionym w poniższej tabeli, które obowiązują do 30.09.2026 r. Zamawiający wymaga, aby świadczenie usługi WAF rozpoczęło się nie wcześniej niż przed 1.10.2026 r.

Obecnie usługa świadczona jest w oparciu o zintegrowaną platformę klasy WAAP, jednego producenta, zarządzanej z poziomu wspólnej konsoli.

L.p.	Numer katalogowy	Produkt	Liczba produktów
1	M-LC-169584	App & API Protector with delivery	1
2	M-LC-160433	Application Load Balancing	1
3	M-LC-161591	API Gateway	1
4	M-LC-62373	Edge DNS	1

IV. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

W ramach zamówienia Wykonawca zobowiązany będzie do:

- udostępnienia platformy ochronnej klasy Web Application Firewall (WAF), w tym:
 - zapewnienia ochrony przed atakami aplikacyjnymi, w tym co najmniej SQL Injection, XSS, CSRF, atakami botowymi oraz atakami DDoS,
 - usługi autorytatywnego DNS,
 - integracji z systemami SIEM i Log Management Zamawiającego,
- do 1.10.2026 r. Wykonawca zapewni dostęp do platformy ochronnej klasy Web Application Firewall (WAF) i skonfiguruje na niej usługi zgodnie z wymaganiami Zamawiającego opisanymi w OPZ.
- W ramach udostępnionej i skonfigurowanej platformy muszą być świadczone usługi obejmujące ochronę ruchu HTTP/HTTPS do aplikacji i interfejsów API wskazanych przez Zamawiającego w wykazie obiektów objętych ochroną.
- Usługami na platformie muszą być objęte obiekty wskazane przez Zamawiającego w załączniku „Wykaz obiektów objętych ochroną”. Każdy obiekt został opisany następującymi danymi:

- a) nazwa obiektu,
 - b) środowisko,
 - c) adres FQDN / domena,
 - d) rodzaj ruchu: aplikacja webowa / API / inne,
 - e) wymagania w zakresie TLS / mTLS,
 - f) średni wolumen ruchu z 30 dni.
5. Każdy obiekt ochrony musi posiadać dedykowany adres usługi, np. publiczny adres IP lub rekord CNAME, na który zostanie skierowany ruch z serwerów DNS Zamawiającego.
 6. Usługa musi umożliwiać rozbudowę obiektów objętych ochroną minimum do 50 sztuk.
 7. W ramach zamówienia Wykonawca zobowiązany jest do:
 - 1) dostarczenia i utrzymania wszystkich komponentów usługi WAF, DNS i Anty-DDoS objętych zakresem zamówienia,
 - 2) utrzymania mechanizmu integracji oraz udostępniania logów do systemów SIEM i Log Management Zamawiającego,
 - 3) utrzymania warstwy infrastruktury, na której świadczona będzie usługa, w tym ewentualnych kolektorów logów, jeżeli będą wymagane do realizacji integracji,
 - 4) przygotowanie raportów miesięcznych oraz dokumentacji technicznej,
 - 5) konfiguracji usług ochrony do momentu zakończenia wdrożenia
 8. Zamawiający po zawarciu umowy zobowiązuje się do:
 - 1) Wskazania osób uprawnionych do przejęcia w utrzymanie warstwy konfiguracji usługi ochrony
 - 2) przekazania wymaganych informacji o chronionych aplikacjach, niezbędnych do konfiguracji ochrony,
 - 3) konfiguracji systemów SIEM/Log Management po stronie własnej infrastruktury w zakresie odbioru danych z udostępnionego mechanizmu integracji oraz udostępniania logów
 9. W okresie trwania usługi, Zamawiający w zakresie utrzymywanych aplikacji będzie uczestniczył w:
 - 1) Aktualizacji i rozwoju konfiguracji mechanizmów ochrony
 - 2) testach funkcjonalnych aplikacji po wdrożeniu zmian w konfiguracji ochrony,
 - 3) weryfikacji wpływu reguł WAF na działanie aplikacji,
 - 4) analizie false positive i false negative
 - 5) analizie zdarzeń w ramach mechanizmów ochrony
 10. Zamawiający potwierdza poprawność działania aplikacji po wdrożeniu zmian lub rollbacku,

Wymagania funkcjonalne i techniczne platformy ochronnej klasy Web Application Firewall (WAF)

1. Wymagane funkcje muszą być realizowane w ramach jednej, zintegrowanej platformy typu WAAP, jednego producenta, zarządzanej z poziomu wspólnej konsoli.
2. Zamawiający nie dopuszcza realizacji wymaganych funkcji poprzez zestawienie niezależnych, samodzielnie integrowanych komponentów. Zaoferowane usługi muszą być komercyjnie dostępnym, aktualnie wspieranym i rozwijanym produktem producenta, objętym wsparciem technicznym producenta z gwarantowanymi czasami reakcji.
3. Wszystkie komponenty wykorzystane do konfiguracji usługi muszą być objęte aktualnym wsparciem producenta i nie mogą znajdować się poza wsparciem typu end-of-life lub end-of-support.
4. Usługi muszą zapewnić możliwość ograniczenia lokalizacji przechowywania i przetwarzania danych operacyjnych oraz logów usługi do terytorium UE/EOG. Usługa musi posiadać aktualne certyfikaty ISO/IEC 27001 oraz SOC 2 Type II, a Wykonawca udostępni Zamawiającemu na żądanie raporty z audytów. Wykonawca zapewni wsparcie techniczne w języku polskim w trybie 24/7 oraz mechanizmy raportowania incydentów wspierające realizację obowiązków Zamawiającego wynikających z ustawy o KSC oraz dyrektywy NIS2.

Ochrona aplikacji i API

1. Usługa musi zapewniać ochronę przed najczęściej występującymi zagrożeniami aplikacyjnymi, w tym co najmniej: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), atakami botowymi, credential stuffing, brute-force i fałszywym ruchem.
2. Ochrona przed atakami botowymi, credential stuffing i brute-force musi być realizowana z wykorzystaniem co najmniej: analizy behawioralnej ruchu, fingerprintingu klienta (przeglądarki/urządzenia), mechanizmów wyzwań (challenge, w tym JS challenge oraz integracja z mechanizmem CAPTCHA) oraz feedów reputacyjnych/threat intelligence dostarczanych i aktualizowanych przez producenta rozwiązania. Wykrywanie nie może opierać się wyłącznie o limitowanie liczby żądań ani o statyczne listy User-Agent.
3. Dla każdej chronionej aplikacji Wykonawca wdroży zestaw bazowych reguł bezpieczeństwa oparty co najmniej o OWASP Core Rule Set w aktualnie wspieranej wersji (nie starszej niż v4) albo o równoważny zestaw reguł producenta.
4. Reguły bazowe oraz sygnatury muszą być aktualizowane automatycznie przez producenta platformy na podstawie prowadzonej przez niego analizy zagrożeń i globalnej telemetrii, bez konieczności ręcznej rekonfiguracji przez Zamawiającego. Wykonawca wskaże gwarantowany czas dostarczenia aktualizacji reguł w odpowiedzi na nowo zidentyfikowane zagrożenia.
5. Usługa musi umożliwiać ochronę interfejsów API, w tym co najmniej: wykrywanie endpointów API, analizę sekwencji żądań, analizę wartości parametrów, ochronę GraphQL, weryfikację tokenów JWT, kluczy API i OAuth 2.0 oraz egzekwowanie pozytywnego modelu bezpieczeństwa na podstawie wykrytego lub dostarczonego schematu OpenAPI v3.
6. Usługa musi umożliwiać blokowanie i ograniczanie ruchu na podstawie geolokalizacji, list adresów IP oraz list wyjątków. Blokady muszą być możliwe do ustawienia czasowo, a system musi umożliwiać ich automatyczne usunięcie po upływie zdefiniowanego czasu. Musi istnieć możliwość wcześniejszego odblokowania na zlecenie Zamawiającego.

Ochrona DDoS:

1. Dostęp do usługi od strony publicznej sieci Internet musi być objęty ciągłą ochroną Anty-DDoS, obejmującą co najmniej warstwy:
 - 1) ataków wolumetrycznych (L3/L4),
 - 2) ataków protokołowych/wyczerpujących stan (L3/L4, np. SYN flood, fragmentacja),
 - 3) ataków na warstwę aplikacji (L7).
2. Mitygacja ataków wolumetrycznych musi być realizowana w sieci Wykonawcy lub w centrach oczyszczania ruchu (scrubbing center) Wykonawcy, powyżej (upstream) punktu styku Zamawiającego z siecią Internet. Mitygacja realizowana wyłącznie po stronie infrastruktury Zamawiającego (on-premise), w której ruch atakujący osiąga łącze styku przed odfiltrowaniem, nie spełnia wymagania.
3. Wykonawca musi dysponować geograficznie rozproszoną infrastrukturą oczyszczania ruchu opartą o co najmniej trzy niezależne lokalizacje (PoP/scrubbing center), w tym co najmniej jedną na terenie Europejskiego Obszaru Gospodarczego.
4. Usługa musi zapewniać pojemność mitygacji (rozumianą jako zdolność oczyszczania ruchu w sieci Wykonawcy, a nie przepustowość łącza styku Zamawiającego) na poziomie nie mniejszym 300 Gbps oraz 200 Mpps.

Dostępność:

1. Usługa musi obsługiwać oba poniższe tryby pracy środowiska podstawowego i zapasowego Zamawiającego, z możliwością konfiguracji wybranego trybu przez Zamawiającego:
 - 1) active-passive — przełączanie awaryjne (failover) ruchu na środowisko zapasowe
 - 2) active-active — jednoczesne rozkładanie ruchu pomiędzy środowiska.
2. Usługa musi umożliwiać przełączanie ruchu pomiędzy środowiskiem podstawowym i zapasowym w oparciu o mechanizm kontroli stanu (health-check) realizowany żądaniami HTTP lub HTTPS.
3. Mechanizm health-check musi umożliwiać konfigurację co najmniej następujących parametrów:
 - 1) interwał odpytywania,

- 2) limit czasu odpowiedzi (timeout),
 - 3) liczba kolejnych nieudanych/udanych prób decydująca o zmianie stanu,
 - 4) kryterium zdrowia: oczekiwany kod odpowiedzi HTTP oraz opcjonalnie dopasowanie treści odpowiedzi,
 - 5) ustawiany nagłówek Host,
 - 6) ustawiana wartość SNI w sondzie HTTPS.
4. Usługa musi umożliwiać rozkładanie ruchu pomiędzy środowiskami z zachowaniem ciągłości sesji (persystencja) co najmniej w oparciu o:
- 1) źródłowy adres IP,
 - 2) wskazany przez Zamawiającego nagłówek HTTP,
 - 3) cookie sesyjne (np. SESSIONID).
5. Usługa musi zapewniać pełną interoperacyjność z urządzeniami i oprogramowaniem równoważącym obciążenie (load balancer) eksploatowanymi w środowisku podstawowym i zapasowym Zamawiającego, w tym z rozwiązaniami klasy Enterprise (m.in. Fortinet FortiWeb, F5 BIG-IP). Współpraca musi obejmować co najmniej:
- 1) przekazywanie rzeczywistego adresu IP klienta do warstwy LB Zamawiającego (nagłówek X-Forwarded-For oraz PROXY protocol v1/v2),
 - 2) poprawne działanie mechanizmu utrzymania sesji (sticky-session) i przekazywanie nagłówków HTTP oraz cookies wykorzystywanych do utrzymania sesji (w tym SESSIONID),
 - 3) poprawne współdziałanie mechanizmu health-check usługi z politykami kontroli stanu LB Zamawiającego, z możliwością ustawienia nagłówka Host oraz wartości SNI w sondzie HTTPS,
 - 4) obsługę przekazywania SNI do warstwy LB Zamawiającego w trybie re- enkrypcji (TLS bridging), bez utraty możliwości selekcji certyfikatu po stronie serwera (server-side SNI),
 - 5) brak konieczności wymiany, przekonfigurowania lub modyfikacji istniejących LB Zamawiającego w sposób naruszający gwarancję lub wsparcie producenta tych urządzeń.
5. Terminacja TLS oraz przechowywanie materiału kryptograficznego muszą odbywać się w lokalizacjach na terenie Europejskiego Obszaru Gospodarczego, zgodnie z wymaganiami suwerenności danych oraz przepisami krajowymi (KSC) i dyrektywą NIS2.

Autorytatywny DNS

1. Usługi autorytatywnego DNS musi Wykonawca świadczyć w oparciu o nie mniej niż cztery serwery autorytatywne DNS, rozumiane jako logiczne punkty dostępowe NS, z których każdy udostępniany jest w technologii anycast (rozproszony na wielu węzłach sieci Wykonawcy), dostępny jednocześnie w protokołach IPv4 oraz IPv6.
2. Usługa musi działać w modelu hidden master. Serwerem nadrzędnym (master) jest serwer Zamawiającego, a serwery udostępnione w ramach usługi pełnią rolę serwerów wtórnych (secondary), pobierających i serwujących strefy opublikowane przez Zamawiającego.
3. Transfer stref (AXFR oraz IXFR) musi posiadać możliwość zabezpieczania kluczem TSIG (RFC 8945) z możliwością wyboru algorytmu nie słabszego niż HMAC- SHA256, ograniczony listą kontroli dostępu (ACL) do adresów Zamawiającego.
4. Wykonawca musi obsługiwać powiadomienia NOTIFY (RFC 1996) inicjowane przez master Zamawiającego.
5. Usługa musi być świadczona w oparciu o rozproszoną, nadmiarowo zwymiarowaną sieć typu anycast, zdolną do absorpcji wolumetrycznych ataków DDoS na warstwę DNS bez degradacji dostępności chronionych stref. Usługa musi obsługiwać chronioną infrastrukturę niezależnie od jej lokalizacji
6. Wykonawca zapewni możliwość ograniczenia lokalizacji przechowywania i przetwarzania danych operacyjnych oraz logów usługi do terytorium UE/EOG. Wykonawca zapewni wsparcie techniczne w języku polskim w trybie 24/7 oraz mechanizmy raportowania incydentów wspierające realizację obowiązków Zamawiającego wynikających z ustawy o KSC oraz dyrektywy NIS2.

Integracja z SIEM i Log Management

1. Wykonawca musi udostępniać logi zdarzeń generowane przez platformę ochronną do systemów SIEM i Log Management Zamawiającego. Integracja musi być realizowana z użyciem powszechnie stosowanych mechanizmów wymiany danych, np. syslog/rsyslog lub równoważnych.
2. Jeżeli do realizacji integracji konieczne będzie wdrożenie maszyny wirtualnej, appliance lub kolektora logów, Wykonawca odpowiada za dostarczenie i utrzymanie tej warstwy w zakresie objętym usługą.
3. Pasma wykorzystywane do przesyłu logów nie może pomniejszać gwarantowanej przepustowości usługi ochrony dla ruchu użytkowników końcowych.

Zarządzanie konfiguracją

1. Wykonawca zapewni Zamawiającemu ciągły dostęp do pełnej, aktualnej konfiguracji aktywnych reguł bezpieczeństwa, obejmującej reguły wbudowane producenta, reguły autorskie oraz parametry tuningu, w formie maszynowo przetwarzalnej, dostępnej zarówno przez interfejs graficzny, jak i przez API (eksport konfiguracji). Udostępnienie nie może być ograniczone do trybu reaktywnego ani uzależnione od jednostkowej oceny zakresu „niezbędnego do audytu”. Konfiguracja musi być dostępna w formie wersjonowanej, umożliwiającej odtworzenie stanu reguł na dowolny moment objęty retencją.
2. Usługa musi umożliwiać:
 - 1) testowanie zmian konfiguracji bez wpływu na ruch produkcyjny (np. tryb detekcji/report albo odrębna warstwa testowa),
 - 2) wersjonowanie konfiguracji z możliwością odtworzenia i przywrócenia (rollback) dowolnej wcześniejszej wersji,
 - 3) aktywację wybranej wersji konfiguracji. Dopuszcza się realizację wersjonowania i rollbacku w oparciu o deklaratywne zarządzanie konfiguracją przez API/IaC, pod warunkiem pełnego pokrycia funkcji konfiguracyjnych przez to API.
3. Pełnia funkcji konfiguracyjnych usługi musi być dostępna deklaratywnie przez udokumentowane, wersjonowane API, w zakresie nie węższym niż dostępny przez GUI, obejmującym co najmniej: reguły WAF, polityki ochrony API, polityki bot management, reguły rate-limiting oraz polityki mitygacji DDoS warstwy aplikacyjnej. Producent rozwiązania musi udostępniać i utrzymywać oficjalny provider Terraform, publikowany w publicznym rejestrze lub udostępniany przez producenta wraz z dokumentacją i wsparciem. Nie dopuszcza się realizacji tego wymogu wyłącznie poprzez autorskie skrypty Wykonawcy, moduły społecznościowe ani mechanizmy „równoważne” nieobjęte wsparciem producenta.

Monitoring, obsługa zgłoszeń i incydentów

Monitoring dostępności

1. Dostępność usługi musi być utrzymywana na poziomie minimum 99,99% w cyklu miesięcznym, co odpowiada maksymalnie 4 minutom i 23 sekundom niedostępności w miesiącu rozliczeniowym.
2. Rozliczenie dostępności będzie oparte o zewnętrzny system monitoringu Zamawiającego, wykonujący testy ciągłe z minimum trzech lokalizacji geograficznie rozdzielonych. Za niedostępność uznaje się niedostępność spowodowaną przez dowolny element dostarczony w ramach usługi ochrony.
3. Do czasu niedostępności nie wlicza się wcześniej uzgodnionych przerw serwisowych zaakceptowanych przez Zamawiającego co najmniej 24 godziny przed ich rozpoczęciem. Łączny czas przerw serwisowych nie może przekroczyć 4 godzin w miesiącu, a prace powinny być prowadzone w godzinach 22:00-4:00. W czasie planowanej przerwy serwisowej Wykonawca publikuje komunikat przekazany przez Zamawiającego.
4. Na potrzeby realizacji umowy stosuje się następujące poziomy zgłoszeń:
 - 1) Błąd krytyczny - niepoprawne działanie usługi uniemożliwiające korzystanie z chronionej aplikacji lub powodujące realne zagrożenie dla bezpieczeństwa, w szczególności całkowitą niedostępność usługi ochrony, całkowitą niedostępność chronionej aplikacji spowodowaną przez usługę ochronną, błędne przetwarzanie ruchu prowadzące do utraty poprawnego działania systemu albo potwierdzony incydent bezpieczeństwa wymagający natychmiastowej reakcji.
 - 2) Błąd poważny - niepoprawne działanie usługi istotnie utrudniające korzystanie z

chronionej aplikacji albo obniżające poziom bezpieczeństwa, ale niepowodujące całkowitej niedostępności.

- 3) Usterka - każda inna nieprawidłowość, która nie spełnia kryteriów błędu krytycznego ani poważnego, w tym niezgodność działania z dokumentacją lub błędy nieblokujące pracy usługi.
5. Czas reakcji i usunięcia
 - 1) W przypadku błędu krytycznego czas reakcji wynosi maksymalnie 0,5 godziny, czas zastosowania obejścia maksymalnie 0,5 godziny, a czas trwałej naprawy maksymalnie 1 godzinę.
 - 2) W przypadku błędu poważnego czas reakcji wynosi maksymalnie 0,5 godziny, czas zastosowania obejścia maksymalnie 1 godzinę, a czas trwałej naprawy maksymalnie 2 godziny.
 - 3) W przypadku usterki czas reakcji wynosi maksymalnie 0,5 godziny, a czas naprawy maksymalnie 24 godziny. Dla usterek nie wymaga się wdrażania obejścia, chyba że Strony uzgodnią inaczej dla konkretnego przypadku.
 - 4) W ramach świadczonej usługi Zamawiający ma prawo do zgłaszania błędów i incydentów przez cały rok, 7 dni w tygodniu, 24 godziny na dobę. Czas reakcji liczony jest od momentu zarejestrowania zgłoszenia.

Zgłoszenia i kanały komunikacji

1. Podstawowym kanałem rejestracji zgłoszeń jest system obsługi incydentów udostępniony przez Zamawiającego. W przypadku niedostępności systemu dopuszcza się zgłoszenia przez e-mail lub telefon, przy czym zgłoszenie telefoniczne wymaga późniejszego potwierdzenia w uzgodnionym kanale komunikacyjnym.
2. Kanały komunikacji obowiązujące w ramach umowy:
 - 1) system obsługi incydentów
 - 2) adres e-mail do zgłoszeń
 - 3) numer telefonu dla zgłoszeń krytycznych
3. Jeżeli awaria lub incydent zostanie wykryty przez Wykonawcę lub przez źródło zewnętrzne, Wykonawca ma obowiązek niezwłocznie rozpocząć działania i zarejestrować zgłoszenie po swojej stronie oraz w systemie Zamawiającego nie później niż w ciągu 0,5 godziny.

Parametry ilościowe i pojemnościowe

1. Minimalna gwarantowana przepustowość łącza obsługującego ochronę obiektów wynosi 2 Gbps.
2. Wymagany dopuszczalny wolumen ruchu do chronionych aplikacji wynosi do 20TB miesięcznie.
3. Wymagana dopuszczalna ilość żądań do chronionych aplikacji wynosi 1 miliard żądań miesięcznie.
4. Wymagane jest obsłużenie nielimitowanej ilości żądań DNS do skonfigurowanych stref DNS.
5. W ramach usługi Zamawiający ma mieć możliwość skonfigurowania do 15 stref DNS które posiadają 1500 rekordów DNS łącznie.