Ministerstwo Rozwoju i Technologii

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na Ochrona przed zagrożeniami z sieci Internet klasy Web Application Firewall (WAF)

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia, tj. Ochrona przed zagrożeniami z sieci Internet klasy Web Application Firewall (WAF) będzie realizowany poprzez:

1. udostępnienie platformy ochronnej klasy Web Application Firewall (WAF),
2. usługi asysty technicznej.

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	24 miesiące
2	M-LC-160433	Application Load Balancing	1	24 miesiące
3	M-LC-161591	API Gateway	1	24 miesiące
4	M-LC-62373	Edge DNS	1	24 miesiące
5	M-LC-170810	Content Protector	1	24 miesiące
6	M-LC-168897	Integrating Akamai products	1	24 miesiące
7	n.d.	Usługi asysty	250	24 miesiące

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w następujących terminach:

1. do 30 dni od podpisania umowy Wykonawca udostępni platformę ochronną klasy Web Application Firewall (WAF) na okres 24 miesięcy,
2. 24 miesiące od dnia udostępnienia skonfigurowanej platformy w zakresie usług asysty technicznej.

Zamawiający przewiduje płatności roczne za pozycje od 1 do 6 wymienione w ww. tabeli.

III. AKTUALNY STAN

1. Zamawiający posiada wdrożone usługi ochrony publicznie dostępnych aplikacji webowych klasy Web Application Firewall (WAF), w zakresie wymienionym w poniższej tabeli.
2. 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
5	M-LC-169844	Managed Security Services 3.0	1
6	M-LC168897	Integrating Akamai products	1

IV. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

W ramach zamówienia Wykonawca zobowiązany będzie do:

1. udostępnienia platformy ochronnej klasy Web Application Firewall (WAF), w tym:
   a) zapewnienia ochrony przed atakami aplikacyjnymi, w tym co najmniej SQL Injection, XSS, CSRF, atakami botowymi oraz atakami DDoS,
   b) usługi autorytatywnego DNS,
   c) integracji z systemami SIEM i Log Management Zamawiającego,
2. do 30 dni od daty podpisania przez strony umowy, w zakresie realizacji zamówienia Wykonawca udostępni oferowaną platformę ochronną klasy Web Application Firewall (WAF) i skonfiguruje na niej usługi zgodnie z wymaganiami Zamawiającego opisanymi w OPZ.
3. W ramach skonfigurowanej platformy muszą być świadczone usługi obejmujące ochronę ruchu HTTP/HTTPS do aplikacji i interfejsów API wskazanych przez Zamawiającego w wykazie obiektów objętych ochroną.
4. 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. Platforma musi umożliwiać rozbudowę obiektów objętych ochroną minimum do 50 sztuk.
7. W ramach zamówienia Wykonawca zobowiązany jest do:
   1) dostarczenia i utrzymania wszystkich komponentów platformy 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 udostępniona jest platforma, w tym ewentualnych kolektorów logów, jeżeli będą wymagane do realizacji integracji,
   4) przygotowanie i przekazywanie raportów miesięcznych oraz dokumentacji technicznej,
   5) konfiguracji usług ochrony do momentu zakończenia instalacji i konfiguracji.
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 obowiązywania umowy, 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 będzie potwierdzał 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.

Ochrona aplikacji i API

1. Platforma 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, zautomatyzowanym scrapingiem i fałszywym ruchem.
2. Ochrona przed atakami botowymi, zautomatyzowanym scrapingiem i fałszywym ruchem 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. Platforma musi zapewniać ochronę przed zaawansowanymi mechanizmami automatycznego pobierania treści (web scraping), w tym przed botami wykorzystującymi przeglądarki bezgłowe, frameworki automatyzujące. Wymagana jest detekcja oparta na analizie behawioralnej ruchu, odciskach palca urządzenia i przeglądarki (fingerprinting) oraz weryfikacji zdolności wykonania kodu JavaScript, bez konieczności modyfikacji kodu chronionych aplikacji. Mechanizm musi wykrywać żądania rozłożone w czasie i o niskiej intensywności
4. Dla każdej chronionej aplikacji Wykonawca uruchomi 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.
5. 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.
6. Platforma musi umożliwiać ochronę interfejsów API, w tym co najmniej:, analizę sekwencji żądań, weryfikację tokenów JWT, kluczy API i OAuth 2.0 oraz egzekwowanie pozytywnego modelu bezpieczeństwa na podstawie wykrytego lub dostarczonego schematu OpenAPI v3.
7. Platforma 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.
8. Platforma musi dostarczać ochronę interfejsów programistycznych (API) oraz punktów końcowych aplikacji Zamawiającego przed nieuprawnionym ruchem automatycznym, realizowana niezależnie dla każdego chronionego punktu końcowego.
9. Platforma musi automatycznie budować i utrzymywać profil bazowy (baseline) ruchu normalnego, odrębnie dla każdej chronionej domeny/aplikacji objętej usługą.
10. Platforma musi obsługiwać automatyczne dostrajanie, aby zachowywać skuteczność w warunkach zmieniających się technik i sygnatur botów, tj. aktualizacja profilu musi następować cyklicznie/ciągle, bez udziału administratora Zamawiającego.
11. Platforma musi udostępniać co najmniej następujące akcje reakcji na wykryty ruch automatyczny: zezwolenie, blokowanie, przekierowanie, podanie treści alternatywnej (odmiennej od treści udostępnianej użytkownikom), wyzwanie (challenge), spowolnienie odpowiedzi (opóźnienie/ograniczenie przepustowości sesji), monitorowanie bez działania (log only).
12. Platforma musi być chroniona za pomocą ochrony AntyDDoS. Niedostępność usług w związku z trwającym atakiem DDoS jest traktowana jako błąd krytyczny.
13. Platforma w ramach własnej ochrony AntyDDoS musi samodzielnie oczyścić ruch. Mitygacja polegająca na przekazaniu ruchu atakującego do infrastruktury Zamawiającego nie spełnia wymagania.
14. Platforma w ramach własnej ochrony AntyDDoS musi być zdolna do odparcia ataków na poziomie nie mniejszym niż 300Gbps oraz 200Mpps.

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 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),
   2) poprawne działanie mechanizmu utrzymania sesji (sticky-session) i przekazywanie 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.
1. Terminacja TLS musi 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 niemniej 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

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 zainstalowanie maszyny wirtualnej, appliance lub kolektora logów, Wykonawca odpowiada za dostarczenie i utrzymanie tej warstwy w zakresie objętym usługą.
3. Pasmo 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 naprawy maksymalnie 1 godzinę.

2) W przypadku błędu poważnego czas reakcji wynosi maksymalnie 0,5 godziny, czas zastosowania obejścia maksymalnie 1 godzinę, a czas 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 zgłoszeń 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 zgłoszeń,

2) adres e-mail do zgłoszeń,

3) numer telefonu dla zgłoszeń krytycznych

3. Jeżeli błąd, usterka 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.

Instalacja i konfiguracja

1. Etap 1 - W terminie 7 dni od podpisania umowy Wykonawca przygotuje harmonogram realizacji instalacji i konfiguracji. Harmonogram musi zawierać:

a. zadania,
b. zakres odpowiedzialności,
c. zależności,
d. uzgodnienia testów do wykonania na każdym z etapów
e. terminy rozpoczęcia i zakończenia,
f. opis formy i szczegółowy zakres dokumentacji.

2. Etap 2 - W terminie 14 dni od podpisania umowy Wykonawca uruchomi usługę ochrony dla wszystkich obiektów ujętych w „Wykaz obiektów objętych ochroną” i udostępni ją do testów. Wykonawca dostarczy dokumentację w uzgodnionym zakresie i formie do weryfikacji przez Zamawiającego.
3. Etap 3 - W terminie 16 dni od odbioru Etapu 2 Wykonawca przeprowadzi, we współpracy z Zamawiającym, przełączenie ruchu produkcyjnego dla obiektów ujętych w „Wykaz obiektów objętych ochroną”. Wykonawca dostarczy ostateczną wersję dokumentacji uwzględniającą wszystkie uwagi Zamawiającego jakie zgłosi do niej od jej otrzymania na Etapie 2 oraz w trakcie trwania Etapu 3.

4. Od momentu odbioru Etapu 3 zaczyna obowiązywać SLA.
5. Każdy etap uznaje się za zakończony wyłącznie po łącznym spełnieniu poniższych warunków:
    1) dostarczenie wymaganych artefaktów,
    2) wykonanie uzgodnionych testów,
    3) usunięcie zgłoszonych uwag,
    4) uzyskanie akceptacji Zamawiającego.
6. Podstawę odmowy akceptacji przez Zamawiającego, uniemożliwiającej odbiór etapu, stanowi wystąpienie co najmniej jednej z poniższych okoliczności:
    a. wystąpienie błędu krytycznego
    b. wystąpienie błędu poważnego wpływającego na ruch produkcyjny lub bezpieczeństwo
    c. brak wymaganej dokumentacji dla danego etapu.

Raportowanie

1. Wykonawca będzie przygotowywał miesięczny raport zbiorczy obejmujący co najmniej:
    1) wykryte zdarzenia/incydenty i czasy ich obsługi,
    2) podjęte działania,
    3) zmiany konfiguracji,
    4) poziom dostępności usługi.
2. Usługa musi umożliwiać generowanie raportów, przegląd danych historycznych przez minimum 90 dni, prezentację danych na dashboardach oraz dostęp przez przeglądarkę internetową.
3. Raporty i dane analityczne muszą być możliwe do udostępnienia co najmniej w formatach PDF, CSV oraz jako surowe logi.

Usługi asysty technicznej

1. Wykonawca zapewni usługi asysty technicznej dla dostarczonej usługi.
2. Usługi w ramach zamówienia będą świadczone zgodnie z zapotrzebowaniem Zamawiającego, każdorazowo na podstawie zleceń uwzględniających uzgodniony z Wykonawcą zakres, liczbę roboczogodzin oraz termin realizacji.
3. W celu ustalenia zakresu Zlecenia Zamawiający dostarczy Wykonawcy opis wymaganej usługi.
4. Wykonawca przedstawi Zamawiającemu w terminie do 5 dni roboczych wycenę pracochłonności usługi wyrażoną w roboczogodzinach oraz wskaże termin jej realizacji.
5. Zakres, sposób oraz termin realizacji zostaną uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
6. Zamawiający zleci Wykonawcy w formie pisemnego zamówienia, realizację usług asysty technicznej.
7. Zlecenie asysty technicznej będzie zawierać zakres usług do wykonania, czasochłonność w roboczogodzinach oraz termin realizacji, uzgodniony wcześniej z Wykonawcą.
8. Wykonanie usługi przez Wykonawcę zostanie zrealizowane zgodnie z przygotowaną przez Wykonawcę i zatwierdzoną przez Zamawiającego wyceną i zakresem dostarczonym przez Zamawiającego.
9. Usługi mogą być świadczone w dwóch formach:
    a) w siedzibie Zamawiającego,
    b) zdalnie, za pośrednictwem szyfrowanego połączenia.
10. Dostęp Wykonawcy do infrastruktury Zamawiającego będzie odbywał się w sposób zabezpieczony kryptograficznie, poprzez szyfrowane połączenie VPN.
11. Po wykonaniu usług Wykonawca zgłosi Zamawiającemu gotowość odbioru, przekaże do odbioru wyniki wykonanej usługi, wraz z dokumentacją, o ile w ramach danego zlecenia wytworzenie dokumentacji było przewidziane.

12. W terminie 10 dni od realizacji przez Wykonawcę danego zlecenia, Zamawiający dokonuje weryfikacji poprawności i zgodności jego wykonania z zakresem wskazanym w zleceniu oraz wyceną Wykonawcy i akceptuje wyniki przedstawionych prac i strony podpisują protokół odbioru albo Zamawiający zgłasza Wykonawcy uwagi do wykonanych prac lub materiałów.
13. W przypadku zgłoszenia przez Zamawiającego uwag, Wykonawca zobowiązany jest do usunięcia niezgodności w terminie wskazanym przez Zamawiającego, nie dłuższym niż 5 dni, bez dodatkowego wynagrodzenia z tego tytułu.
14. Po poprawienia zgodnie ze zgłoszonymi uwagami Wykonawca ponownie zgłosi do odbioru Zamawiającemu wykonanie danego zlecenia. Do jego odbioru stosuje się odpowiednio zapisy wskazane w pkt 11 i 12.
15. Maksymalna liczba roboczogodzin przewidziana w zamówieniu wynosi 250 roboczogodzin.
16. Zamawiający zastrzega sobie prawo do niewykorzystania maksymalnej liczby roboczogodzin.
17. Zamawiający ma prawo do rezygnacji z realizacji danego zlecenia bez podania przyczyny.

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 25TB 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.

V. MIEJSCE I TERMIN SKŁADANIA WYCEN

1. Ofertę należy przesłać **do dnia 22.09.2026 r. do godz. 13.00**.
2. Oferty należy przesłać za pośrednictwem poczty elektronicznej poprzez wypełnienie załączonego Formularza wyceny szacunkowej, stanowiącego załącznik do niniejszego zapytania na adres e-mail: ofertyIT@mrit.gov.pl.
3. Cena oferty powinna uwzględniać wszystkie zobowiązania, musi być podana w walucie polskiej, tj. PLN cyfrowo, wraz z należytym podatkiem VAT – jeżeli występuje.

VI. ZAŁĄCZNIKI

1. Załącznik – Formularz wyceny szacunkowej