OPIS PRZEDMIOTU ZAMÓWIENIA

Usługa ochrony publicznie dostępnych aplikacji webowych z wykorzystaniem WAF, ochrony Anty-DDoS oraz usługi autorytatywnego DNS

1 Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie, uruchomienie, konfiguracja, utrzymanie i rozwój usługi ochrony publicznie dostępnych aplikacji Zamawiającego z wykorzystaniem rozwiązania klasy Web Application Firewall (WAF), ochrony Anty-DDoS oraz usługi autorytatywnego DNS. Usługa obejmuje ochronę ruchu HTTP/HTTPS do aplikacji i interfejsów API wskazanych przez Zamawiającego w wykazie obiektów objętych ochroną.

Zakres zamówienia obejmuje w szczególności:

- dostarczenie i uruchomienie platformy ochronnej WAF,
- zapewnienie ochrony przed atakami aplikacyjnymi, w tym co najmniej SQL Injection, XSS, CSRF, atakami botowymi oraz atakami DDoS,
- dostarczenie usługi autorytatywnego DNS,
- integrację z systemami SIEM i Log Management Zamawiającego,
- bieżące utrzymanie, monitoring, analizę zdarzeń i obsługę incydentów bezpieczeństwa,
- wdrażanie, testowanie i aktualizację reguł bezpieczeństwa, w tym reguł dedykowanych dla chronionych aplikacji,
- raportowanie operacyjne i bezpieczeństwa,
- wsparcie techniczne, warsztaty oraz usługi inżynierskie w trakcie obowiązywania umowy.

2 Zakres obiektów objętych ochroną

2.1 Usługa obejmuje obiekty wskazane przez Zamawiającego w załączniku „Wykaz obiektów objętych ochroną”. Każdy obiekt został opisany następującymi danymi:
- 2.1.1 nazwa obiektu,
- 2.1.2 środowisko,
- 2.1.3 adres FQDN / domena,
- 2.1.4 rodzaj ruchu: aplikacja webowa / API / inne,
- 2.1.5 wymagania w zakresie TLS / mTLS,
- 2.1.6 średni wolumen ruchu z 30 dni,

2.2 Każdy obiekt ochrony musi posiadać dedykowany adres usługi, np. publiczny adres IP lub rekord CNAME, na który zostanie skierowany ruch z serwerów DNS Zamawiającego.

2.3 Dostarczona usługa musi obejmować możliwość rozbudowy obiektów objętych ochroną do 50 sztuk.

3 Granice odpowiedzialności stron

3.1 Wykonawca odpowiada za:

- 3.1.1 dostarczenie i utrzymanie wszystkich komponentów usługi WAF, DNS i Anty-DDoS objętych zakresem zamówienia,
- 3.1.2 konfigurację, utrzymanie, monitoring i rozwój reguł bezpieczeństwa,
- 3.1.3 analizę zdarzeń i incydentów w obszarze dostarczonego rozwiązania,
- 3.1.4 integrację oraz udostępnienie logów do systemów SIEM i Log Management Zamawiającego,
- 3.1.5 przygotowanie, testowanie i wdrażanie zmian w konfiguracji ochrony,
- 3.1.6 utrzymanie warstwy infrastruktury dostarczonej w ramach usługi, w tym ewentualnych kolektorów logów, jeżeli będą wymagane do realizacji integracji,
- 3.1.7 przygotowanie raportów miesięcznych, raportów incydentowych oraz dokumentacji technicznej,
- 3.1.8 realizację testów wymaganych przed odbiorem i po wdrożeniu.

3.2 Zamawiający odpowiada za:

- 3.2.1 przekazanie wykazu obiektów objętych ochroną,
- 3.2.2 wskazanie osób uprawnionych do zgłoszeń, akceptacji zmian i odbiorów,
- 3.2.3 przekazanie wymaganych informacji o chronionych aplikacjach, niezbędnych do konfiguracji ochrony,

3.2.4 udostępnienie systemów SIEM / Log Management po stronie własnej infrastruktury, jeżeli integracja ma być realizowana do tych systemów,
3.2.5 akceptację harmonogramów, dokumentacji, zmian i odbiorów etapów,
3.2.6 dostarczenie treści komunikatów planowanych przerw serwisowych publikowanych dla użytkowników końcowych.

3.3 Podmioty utrzymujące aplikacje odpowiadają za:

3.3.1 wsparcie testów funkcjonalnych aplikacji po wdrożeniu zmian w konfiguracji ochrony,
3.3.2 weryfikację wpływu reguł WAF na działanie aplikacji,
3.3.3 potwierdzanie poprawności działania aplikacji po wdrożeniu zmian lub rollbacku,
3.3.4 udział w analizie false positive i false negative, jeżeli problem dotyczy logiki aplikacji.

4 Wymagania funkcjonalne i techniczne

4.1 Wymagania ogólne dla platformy

4.1.1 Wymagane funkcje muszą być realizowane w ramach jednej, zintegrowanej platformy klasy WAAP jednego producenta, zarządzanej z poziomu wspólnej konsoli, a nie poprzez zestawienie niezależnych, samodzielnie integrowanych komponentów. Rozwiązanie musi być komercyjnie dostępnym, aktualnie wspieranym i rozwijanym produktem producenta, objętym wsparciem technicznym producenta z gwarantowanymi czasami reakcji.
4.1.2 Wszystkie komponenty wykorzystane do budowy usługi muszą być objęte aktualnym wsparciem producenta i nie mogą znajdować się poza wsparciem typu end-of-life lub end-of-support.
4.1.3 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.
4.1.4 Na żądanie Zamawiającego Wykonawca, w terminie 5 dni roboczych, dostarczy działające konto testowe z uprawnieniami umożliwiającymi weryfikację wszystkich funkcji wymaganych w OPZ oraz pełną dokumentację oferowanego rozwiązania.
4.1.5 Środowisko testowe służy wyłącznie weryfikacji dostępności i poprawności działania funkcji wymaganych w OPZ oraz kompletności dokumentacji. Na środowisku testowym nie będzie uruchamiany ruch produkcyjny jakichkolwiek aplikacji Zamawiającego.

4.2 Ochrona aplikacji i API

4.2.1 Rozwiązanie 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.
4.2.2 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.
4.2.3 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.
4.2.4 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.
4.2.5 Producent platformy musi posiadać udokumentowany, działający zespół badawczy w obszarze bezpieczeństwa aplikacyjnego, odpowiedzialny za rozwój reguł i sygnatur.

4.2.6 Dla każdej chronionej aplikacji Wykonawca przygotuje i będzie utrzymywał reguły dedykowane, oparte o analizę ruchu, charakter aplikacji oraz identyfikowane ryzyka. Reguły dedykowane muszą być rozwijane w trybie ciągłym, a ich planowy przegląd musi być wykonywany nie rzadziej niż 4 razy w roku. Analiza pogłębiona może być uruchamiana również na żądanie Zamawiającego, w szczególności w związku z uruchomieniem nowych modułów lub zmianą funkcjonalną aplikacji.

4.2.7 Rozwiązanie 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.

4.2.8 Rozwiązanie 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.

4.3 Ochrona DDoS i dostępność

4.3.1 Dostęp do usługi od strony publicznej sieci Internet musi być objęty ciągłą ochroną Anty-DDoS, obejmującą co najmniej warstwy:

4.3.1.1 ataków wolumetrycznych (L3/L4),

4.3.1.2 ataków protokołowych / wyczerpujących stan (L3/L4, np. SYN flood, fragmentacja),

4.3.1.3 ataków na warstwę aplikacji (L7)

4.3.2 Wykonawca musi zapewnić całodobowy nadzór operacyjny (zespół typu SOC/NOC w trybie 24/7/365) odpowiedzialny za detekcję, reakcję i mitygację incydentów bezpieczeństwa typu DDoS oraz dostępności usługi.

4.3.3 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 infrastructury Zamawiającego (on-premise), w której ruch atakujący osiąga łącze styku przed odfiltrowaniem, nie spełnia wymagania.

4.3.4 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.

4.3.5 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.

4.3.6 Usługa musi być oparta o co najmniej dwa niezależne połączenia internetowe dostarczane przez różnych operatorów (różne podmioty z różnymi systemami autonomicznymi AS).

4.3.7 Łącza muszą być wzajemnie niezależne pod względem ryzyka współdzielonego losu. W szczególności nie mogą korzystać z tej samej kanalizacji teletechnicznej na całym przebiegu, tego samego pojedynczego punktu wymiany ruchu (IX) jako jedynej drogi tranzytu ani tego samego pojedynczego operatora nadrzędnego (upstream) jako jedynego dostawcy tranzytu.

4.3.8 W przypadku awarii jednego z łączy przełączenie ruchu na łącze sprawne musi nastąpić automatycznie, bez ingerencji operatorskiej. Maksymalny czas przełączenia (RTO na poziomie warstwy sieciowej) nie może przekraczać 30 sekund.

4.3.9 Usługa musi obsługiwać oba poniższe tryby pracy środowiska podstawowego i zapasowego Zamawiającego, z możliwością konfiguracji wybranego trybu przez Zamawiającego:

4.3.9.1 active-passive — przełączanie awaryjne (failover) ruchu na środowisko zapasowe

4.3.9.2 active-active — jednoczesne rozkładanie ruchu pomiędzy środowiska.

4.3.10 Usługa musi umożliwiać przełączanie ruchu pomiędzy środowiskiem podstawowym i zapasowym w oparciu o mechanizm kontroli stanu (health-check) realizowany żądaniami HTTP lub HTTPS.

4.3.11 Mechanizm health-check musi umożliwiać konfigurację co najmniej następujących parametrów:

4.3.11.1 interwał odpytywania,

4.3.11.2 limit czasu odpowiedzi (timeout),

4.3.11.3 liczba kolejnych nieudanych/udanych prób decydująca o zmianie stanu,

4.3.11.4 kryterium zdrowia: oczekiwany kod odpowiedzi HTTP oraz opcjonalnie dopasowanie treści odpowiedzi,
4.3.11.5 ustawiany nagłówek Host,
4.3.11.6 ustawiana wartość SNI w sondzie HTTPS.

4.3.12 Usługa musi umożliwiać rozkładanie ruchu pomiędzy środowiskami z zachowaniem ciągłości sesji (persystencja) co najmniej w oparciu o:
4.3.12.1 źródłowy adres IP,
4.3.12.2 wskazany przez Zamawiającego nagłówek HTTP,
4.3.12.3 cookie sesyjne (np. SESSIONID)

4.3.13 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:
4.3.13.1 przekazywanie rzeczywistego adresu IP klienta do warstwy LB Zamawiającego (nagłówek X-Forwarded-For oraz PROXY protocol v1/v2),
4.3.13.2 zachowanie i przekazywanie nagłówków HTTP oraz cookies wykorzystywanych do utrzymania sesji (w tym SESSIONID),
4.3.13.3 poprawne współdziałanie mechanizmu health-check usługi z politykami kontroli stanu LB Zamawiającego, z możliwością ustawienia nagłówka Host oraz wartości SNI w sondzie HTTPS,
4.3.13.4 obsługę przekazywania SNI do warstwy LB Zamawiającego w trybie re-enkrypcji (TLS bridging), bez utraty możliwości selekcji certyfikatu po stronie serwera (server-side SNI),
4.3.13.5 brak konieczności wymiany, przekonfigurowania lub modyfikacji istniejących LB Zamawiającego w sposób naruszający gwarancję lub wsparcie producenta tych urządzeń.

4.3.14 W zakresie, w jakim świadczenie usługi (utrzymanie sesji L7, server-side SNI) wymaga terminacji TLS, Wykonawca musi jednoznacznie opisać miejsce terminacji oraz sposób przechowywania i ochrony kluczy prywatnych i certyfikatów.

4.3.15 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.

4.3.16 Wykonawca musi umożliwić model zarządzania kluczami zapewniający Zamawiającemu kontrolę nad materiałem kryptograficznym (np. BYOK lub przechowywanie kluczy w module HSM); szczegółowy model podlega uzgodnieniu na etapie wdrożenia.

4.4 Autorytatywny DNS

4.4.1 W ramach usługi Wykonawca dostarczy nie mniej niż cztery (4) 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.

4.4.2 Usługa działa 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.

4.4.3 Transfer stref (AXFR oraz IXFR) musi musi posiadać możliwość zabezpieczonia kluczem TSIG (RFC 8945) z możliwością wyboru algorytmu nie słabszego niż HMAC-SHA256, ograniczony listą kontroli dostępu (ACL) do adresów Zamawiającego.

4.4.4 Wykonawca musi obsługiwać powiadomienia NOTIFY (RFC 1996) inicjowane przez master Zamawiającego.

4.4.5 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

4.4.6 Wykonawca zapewni 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.

4.5 Integracja z SIEM i Log Management

4.5.1 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.

4.5.2 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.

4.5.3 Pasmo wykorzystywane do przesyłu logów nie może pomniejszać gwarantowanej przepustowości usługi ochrony dla ruchu użytkowników końcowych.

4.6 Zarządzanie konfiguracją

4.6.1 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.

4.6.2 Rozwiązanie musi umożliwiać:

4.6.2.1 testowanie zmian konfiguracji bez wpływu na ruch produkcyjny (np. tryb detekcji/report albo odrębna warstwa testowa),

4.6.2.2 wersjonowanie konfiguracji z możliwością odtworzenia i przywrócenia (rollback) dowolnej wcześniejszej wersji,

4.6.2.3 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.

4.6.3 „oficjalny, utrzymywany przez producenta provider Terraform (publikowany w publicznym rejestrze lub udostępniany przez producenta wraz z dokumentacją i wsparciem)" — żeby nie wyciąć Link11, jeśli ich provider nie jest w publicznym rejestrze, a jednocześnie nie wpuścić autorskiego skryptu Wykonawcy.

4.6.4 Pełnia funkcji konfiguracyjnych rozwiązania 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.

5 Monitoring, obsługa zdarzeń i incydentów

5.1 Monitoring dostępności

5.1.1 Wykonawca jest zobowiązany do ciągłego monitorowania dostępności dostarczonego rozwiązania oraz do reagowania na incydenty wpływające na działanie usługi.

5.1.2 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.

5.1.3 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.

5.1.4 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.

5.2 Na potrzeby realizacji umowy stosuje się następujące klasy:

5.2.1 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.

5.2.2 Błąd poważny – niepoprawne działanie usługi istotnie utrudniające korzystanie z chronionej aplikacji albo obniżające poziom bezpieczeństwa, ale niepowodujące całkowitej niedostępności.

5.2.3 Usterka – każda inna nieprawidłowość, która nie spełnia kryteriów błędu krytycznego ani poważnego, w tym niezgodność działania z dokumentacją lub błędy nieblokujące pracy usługi.

5.3 Czas reakcji i usunięcia

5.3.1 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.

5.3.2 W przypadku błędu poważnego czas reakcji wynosi maksymalnie 0,5 godziny, czas zastosowania obejścia maksymalnie 1 godzinę, a czas trwałej naprawy maksymalnie 2 godziny.

5.3.3 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.

5.4 Tryb pracy operacyjnej

5.4.1 Zamawiający ma prawo zgłaszać błędy i incydenty przez cały rok, 7 dni w tygodniu, 24 godziny na dobę. Czas reakcji liczony jest od momentu zarejestrowania zgłoszenia.

5.4.2 Wykonawca zapewnia ciągłą gotowość operacyjną do obsługi błędów krytycznych i poważnych oraz incydentów bezpieczeństwa klasy krytycznej i wysokiej. Dla zdarzeń średnich i niskich dopuszcza się analizę planową, jednak nie rzadziej niż raz na 24 godziny. Wymóg przeglądu alertów nie rzadziej niż co 24 godziny pozostaje obowiązkowy.

5.5 False positive / false negative

5.5.1 Jeżeli reguła bezpieczeństwa błędnie blokuje poprawny ruch użytkownika lub aplikacji, zdarzenie jest traktowane jako false positive i obsługiwane co najmniej jako błąd poważny, a jeżeli skutkuje całkowitą niedostępnością usługi – jako błąd krytyczny.

5.5.2 Jeżeli usługa nie zablokowała ruchu, który powinien zostać zaklasyfikowany jako atak, zdarzenie jest traktowane jako false negative i podlega analizie bezpieczeństwa, korekcie reguł oraz raportowi przyczynowemu.

5.5.3 Dla obu przypadków Wykonawca przygotowuje analizę przyczyny, rekomendację zmiany i plan wdrożenia korekty.

6 Zgłoszenia i kanały komunikacji

6.1 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 trwałym. Kanały komunikacji operacyjnej obowiązujące w ramach umowy:

6.1.1 system obsługi incydentów

6.1.2 adres e-mail do zgłoszeń

6.1.3 numer telefonu dla zgłoszeń krytycznych

6.2 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.

7 Zarządzanie zmianą

7.1 Każda zmiana konfiguracji ochrony musi być realizowana w jednym z trzech trybów: zmiana standardowa, zmiana pilna, zmiana awaryjna. Dla każdej zmiany Wykonawca przygotowuje co najmniej:
- 7.1.1 opis zakresu zmiany,
- 7.1.2 powód zmiany,
- 7.1.3 ocenę wpływu na dostępność i bezpieczeństwo,
- 7.1.4 plan testów,
- 7.1.5 plan rollbacku,
- 7.1.6 termin wdrożenia,
- 7.1.7 wskazanie osoby zatwierdzającej po stronie Zamawiającego.

7.2 Zmiany awaryjne, których celem jest natychmiastowa mitygacja aktywnego ataku lub usunięcie błędu krytycznego, mogą zostać wdrożone przed formalną akceptacją, pod warunkiem niezwłocznego poinformowania Zamawiającego i uzupełnienia dokumentacji po wdrożeniu.

8 Wymagania wdrożeniowe

8.1 W ramach oferty Wykonawca przedstawi harmonogram ramowy zawierający główne etapy i kamienie milowe.

8.2 W terminie 14 dni od podpisania umowy Wykonawca przygotuje harmonogram szczegółowy podlegający akceptacji Zamawiającego. Harmonogram musi zawierać zadania, odpowiedzialności, zależności, terminy rozpoczęcia i zakończenia oraz plan aktualizacji dokumentacji.

8.3 W terminie 30 dni od podpisania umowy Wykonawca uruchomi usługę wraz z kandydacką konfiguracją i udostępni ją do testów. Konfiguracja ta musi zapewniać ochronę krytycznych funkcji ruchu zgodnie z wymaganiami podstawowymi.

8.4 W terminie 14 dni od dostarczenia środowiska testowego Wykonawca udostępni środowisko produkcyjne i przeprowadzi, we współpracy z Zamawiającym, przełączenie ruchu produkcyjnego. Od momentu przełączenia zaczyna obowiązywać rygor SLA.

8.5 Najpóźniej 1 dzień przed zakończeniem etapu uruchomienia produkcyjnego Wykonawca dostarczy dokumentację techniczną obejmującą architekturę, parametry techniczne, schematy, zasady utrzymania i rozwoju rozwiązania. Forma i szczegółowy zakres dokumentacji zostaną uzgodnione z Zamawiającym.

8.6 W terminie 120 dni od uruchomienia usługi produkcyjnej Wykonawca przeprowadzi pogłębioną analizę ruchu i logów, przygotuje konfigurację docelową, udostępni ją w środowisku testowym i wdroży zaakceptowane zmiany na produkcji dla wszystkich chronionych aplikacji.

8.7 W terminie 45 dni od uruchomienia konfiguracji po analizie pogłębionej Wykonawca wykona testy i walidację oraz przekaże raporty z tych działań Zamawiającemu.

8.8 Jeżeli Zamawiający zgłosi potrzebę uruchomienia integracji z SIEM i Log Management, Wykonawca w terminie 14 dni przygotuje i uzgodni harmonogram prac, a sama realizacja nie może trwać dłużej niż 30 dni roboczych od zatwierdzenia harmonogramu.

8.9 Każdy etap uznaje się za zakończony wyłącznie po łącznym spełnieniu poniższych warunków:
- 8.9.1 dostarczenie wymaganych artefaktów,
- 8.9.2 wykonanie uzgodnionych testów,
- 8.9.3 usunięcie błędów blokujących odbiór,
- 8.9.4 przekazanie protokołu odbioru,
- 8.9.5 akceptacja Zamawiającego.

8.10 Błędem blokującym odbiór jest każdy błąd krytyczny, każdy błąd poważny wpływający na ruch produkcyjny lub bezpieczeństwo oraz brak wymaganej dokumentacji dla danego etapu.

9 Testy i walidacja

9.1 Wykonawca przeprowadzi testy funkcjonalne, niefunkcjonalne, wydajnościowe, obciążeniowe, bezpieczeństwa oraz testy mechanizmów redundancji i przełączania.

9.2 Wykonawca przeprowadzi symulacje ataków obejmujące co najmniej SQL Injection, XSS, CSRF i DDoS.

9.3 Wykonawca zleci testy penetracyjne zewnętrznemu, wyspecjalizowanemu podmiotowi bez dodatkowych kosztów dla Zamawiającego.

9.4 Wyniki wszystkich testów muszą zostać udokumentowane i przekazane Zamawiającemu w ramach odbioru.
9.5 Zamawiający zastrzega sobie prawo do samodzielnego przeprowadzania testów bezpieczeństwa i wydajności po uprzednim powiadomieniu Wykonawcy co najmniej 2 dni robocze wcześniej.

10 Raportowanie

10.1 Wykonawca będzie przygotowywał miesięczny raport zbiorczy obejmujący co najmniej:
10.1.1 wykryte zdarzenia i incydenty,
10.1.2 podjęte działania,
10.1.3 zmiany konfiguracji,
10.1.4 dostępność usługi,
10.1.5 rekomendacje dotyczące dalszego utrzymania i rozwoju.

10.2 Rozwiązanie musi umożliwiać generowanie raportów, przegląd danych historycznych przez minimum 90 dni, prezentację danych na dashboardach oraz dostęp przez przeglądarkę internetową.

10.3 Raporty i dane analityczne muszą być możliwe do udostępnienia co najmniej w formatach PDF, CSV oraz jako surowe logi.
10.4 Dla każdego incydentu bezpieczeństwa wymagającego analizy Wykonawca przygotuje raport incydentowy zawierający: opis zdarzenia, czas wykrycia, czas reakcji, zakres wpływu, przyczynę, działania podjęte, rekomendacje oraz dowody techniczne.
10.5 Jeżeli incydent dotyczy danych osobowych lub ryzyka ich naruszenia, raport musi zawierać ocenę wpływu na bezpieczeństwo danych osobowych.

11 Wsparcie i usługi dodatkowe

11.1 Wykonawca zapewni pełne wsparcie techniczne i serwisowe dla dostarczonego rozwiązania, w tym aktualizacje oprogramowania, poprawki bezpieczeństwa i doradztwo techniczne.

11.2 Wykonawca przeprowadzi warsztaty dla personelu IT Zamawiającego na żądanie, nie częściej niż dwa razy w roku kalendarzowym, w formie online, z możliwością rejestracji i udostępnienia nagrania. Warsztaty mają być prowadzone dla maksymalnie 5 administratorów i trwać nie krócej niż 8 godzin lekcyjnych.
11.3 Wykonawca zapewni wsparcie inżynierskie w wymiarze 25 godzin na każdy kwartał obowiązywania umowy. Godziny te obejmują konfigurację, optymalizację, analizę i doradztwo dotyczące dostarczonego rozwiązania. Niewykorzystane godziny nie przechodzą na kolejny okres.

12 Parametry ilościowe i pojemnościowe

12.1 Minimalna gwarantowana przepustowość łącza obsługującego ochronę obiektów wynosi 2 Gbps.

12.2 Wymagany dopuszczalny wolumen ruchu do chronionych aplikacji wynosi do 25TB miesięcznie
12.3 Wymagana dopuszczalna ilość żądań do chronionych aplikacji wynosi 1 miliard żądań miesięcznie.
12.4 Wymagane jest obsłużenie nielimitowanej ilości żądań DNS do skonfigurowanych stref DNS.

12.5 W ramach usługi Zamawiający ma mieć możliwość skonfigurowania do 15 stref DNS które posiadają 1500 rekordów DNS łącznie.

13 Wsparcie techniczne systemu:

Wsparcie techniczne musi zapewniać całodobowy nadzór nad bezpieczeństwem środowiska, obsługę incydentów, stały tunning i proaktywny threat hunting. Usługa ta musi również zawierać polskojęzyczny SOC, odpowiedzialny za odpieranie ataków.

13.1 SOC musi być polskojęzyczny, dostarczony bezpośrednio przez VENDORA z referencjami ochrony globalnych ataków każdego dnia.

13.2 Usługa musi zawierać 24/7 monitoring oraz natychmiastową reakcję na incydenty.

13.3 Dodatkowo: przygotowanie na wypadek ataków: techniczny przegląd bezpieczeństwa, kontrola stanu bezpieczeństwa, ćwiczenie gotowości operacyjnej.

13.4 Cały zespół wsparcia musi być polskojęzyczny, a zgłaszanie incydentów musi być dostępne 24/7 poprzez drogę elektroniczną, telefon oraz platformę Dostawcy.

13.5 Wsparcie serwisu – kontrola konta co dwa tygodnie, przypisany polskojęzyczny ekspert ds.bezpieczeństwa, comiesięczne raporty, przegląd biznesowy - zarządzanie zdarzeniami dot.Bezpieczeństwa: proaktywne wsparcie.

13.6 24/7 SOCC, SLA dla Severity 1 = 30 min, raporty po zdarzeniu - proaktywny monitoring – 24/7 monitoring i detekcja anomalii.