Załącznik Nr 4

Urządzenie klasy WAF – rozwiązanie do zabezpieczenia serwerów internetowych, aplikacji i interfejsów API

Opis przedmiotu szacowania:

Minimalne parametry techniczne i funkcjonalne:

1. **Specyfikacja**
   1) System musi być dostarczony w formie hardware, o wysokości maksymalnie 1U(elementy mocujące w zestawie).
   2) Proponowane rozwiązanie musi obsługiwać przepustowość HTTP 0.6 Gbps
   3) Proponowane rozwiązanie musi obsługiwać minimum 1600 nowych sesji HTTP
   4) Proponowane rozwiązanie musi obsługiwać minimum 2400 HTTP Transactions Per Second (TPS)
   5) Proponowane rozwiązanie musi posiadać co najmniej 480 GB pamięci dyskowej
   6) System musi posiadać przynajmniej 2 porty USB, wykorzystywane do podłączania urządzeń zewnętrznych w celu gromadzenia na nich logów
   7) System musi posiadać port typu CON, w celu zarządzania rozwiązaniem z poziomu linii poleceń, gdy dostęp po IP jest niemożliwy.
   8) System musi posiadać dedykowany port do celów zarządzania, nie gorszy niż GE.
   9) System musi posiadać minimalnie 8 interfejsów GE.
   10) System musi posiadać minimum 4GB pamięci RAM.
   11) Proponowane rozwiązanie musi chronić minimum 8 podłączonych aplikacji Web.
   12) Proponowane rozwiązanie musi zabezpieczać minimum 64 pary IP/PORT.
   13) Proponowane rozwiązanie musi obsługiwać RESTful API.
2. **Ochrona aplikacji internetowych**
   1) Proponowane rozwiązanie musi obsługiwać ochronę przed nieprawidłowościami protokołu HTTP.
   2) Proponowane rozwiązanie musi obsługiwać transparentne SSL proxy, które może chronić stronę HTTPS.
   3) Proponowane rozwiązanie musi obsługiwać transparentne SSL proxy, które może chronić tajne strony krajowe HTTPS, a jedna strona może jednocześnie chronić tajne i komercyjne strony internetowe.
   4) Proponowane rozwiązanie musi wspierać ochronę przed atakiem Fast HTTP Flood i powolnym atakiem HTTP Flood.
   5) Proponowane rozwiązanie musi obsługiwać HTTP Flooding - ochrona przed atakami Brute Force obejmująca wiele metod, takich jak statystyki użytkowników, kody weryfikacyjne, ograniczanie szybkości itp.
   6) Proponowane rozwiązanie musi obsługiwać funkcje ataku/obrony wstrzykiwania, które mogą chronić przed SQL injection, LDAP injection, wstrzyknięciami poleceń SSI, wstrzyknięciami Xpath, Remote File Inclusion (RFI) i innymi.
   7) Proponowane rozwiązanie musi obsługiwać funkcje Cross Site Attack/Defense i może bronić przed atakami XSS i CSRF.
   8) Proponowane rozwiązanie musi obsługiwać możliwości inteligentnego wykrywania semantycznego dla ataków SQL injection i XSS.
   9) Proponowane rozwiązanie musi obsługiwać konfigurację różnej czułości reguły wykrywania wstrzykiwania XSS/SQL w celu ochrony przed różnymi poziomami zagrożeń i poprawy dokładności wykrywania.
   10) Obsługa możliwości zapobiegania wyciekom informacji, co może zapobiec wyciekowi informacji, takich jak błędy serwera, błędy bazy danych, zawartość katalogu internetowego, kody programów, słowa kluczowe itp.
   11) Obsługa funkcji zapobiegania wyciekom poufnych informacji. Musi wykryć wyciek osobistych informacji identyfikacyjnych w tym numery identyfikacyjne, numer karty bankowej, numer karty kredytowej i konta e-mail, a także obsługę odczulania poufnych informacji (zastępując je określonymi znakami).
   12) Obsługa możliwości ochrony plików cookie. Musi zapobiec złośliwej ingerencji lub porwaniu plików cookie. Obsługuje również podpisy plików cookie i funkcje szyfrowania.
   13) Proponowane rozwiązanie musi mieć funkcje kontroli dostępu do sieci, które mogą chronić przed skanowaniem, crawlingiem , a także chronić przed zachowaniem directory traversal. Wsparcie ochrony skanowania w oparciu o statystyki behawioralne.
   14) Obsługa precyzyjnej kontroli dostępu HTTP w oparciu o adres IP klienta, który jest w stanie dopasować kryteria, takie jak metoda działania HTTP, nazwa nagłówka HTTP, typ zawartości HTTP, wersja protokołu HTTP, ścieżka URI itp.
   15) Proponowane rozwiązanie musi obsługiwać funkcje ochrony przed lukami w zabezpieczeniach, które są przeznaczone dla serwerów WWW, frameworków internetowych i aplikacji internetowych.
   16) Proponowane rozwiązanie musi mieć możliwość obrony przed nielegalnym dostępem do zasobów,

nielegalnym uploadem/pobieraniem oraz atakami typu hotlink. Wsparcie kontroli dostępu do nielegalnych pobrań w oparciu o rozmiar pliku i typ pliku MIME.

17) Proponowane rozwiązanie musi mieć możliwości ochrony przed złośliwym oprogramowaniem i może bronić się przed Web Shell, atakami koni trojańskich itp.
18) Proponowane rozwiązanie musi mieć zdolność zapobiegania atakom siłowym.
19) Proponowane rozwiązanie musi być w stanie rozpoznać źródłowy adres IP (obsługa atrybutu X-Forward-For) po wdrożeniu za urządzeniem równoważącym obciążenie / serwerem proxy i zablokować rzeczywisty adres IP klienta
20) Proponowane rozwiązanie musi obsługiwać reguły zdefiniowane przez użytkownika.
21) Musi zawierać wstępnie zdefiniowane i niestandardowe szablony polityk zabezpieczeń.
22) Obsługa aktualizacji bazy sygnatur w czasie rzeczywistym.
23) Obsługa funkcji wykrywania i ochrony bezpieczeństwa API. Wsparcie zgodność w oparciu o standardy specyfikacji interfejsu OpenAPI.
24) Możliwość skonfigurowania stanu strony internetowej jako stanu konserwacji witryny.
25) Proponowane rozwiązanie musi obsługiwać wsadową modyfikację konfiguracji witryny (stan witryny, polityka bezpieczeństwa i alarm, status logów dostępu do sieci web, polityka bezpieczeństwa web).
26) Proponowane rozwiązanie musi obsługiwać tryb ponownej ochrony, zapewniać odpowiednie kreatory konfiguracji oraz poprawiać wydajność działania i konserwacji bezpieczeństwa podczas ćwiczeń ofensywnych i defensywnych.

3. **Wykrywanie manipulacji w sieci web**
   1) Obsługa dwóch trybów pracy: trybu uczenia się i trybu ochrony.
   2) Obsługa porównywania chronionych treści na podstawie podobieństwa.
   3) Proponowane rozwiązanie musi obsługiwać niestandardową ochronę statycznych stron sieci Web. Możliwość wykluczenia wyjątku listy adresów URL z ochrony przed manipulacją. Obsługa funkcji planowania.
   4) Obsługa wbudowanego silnika synchronizacji w celu synchronizacji zawartości z serwerów internetowych i ustanowienia linii bazowej.
   5) Obsługa sabotażu i normalnego monitorowania modyfikacji.
   6) Wsparcie kryminalistyki w zakresie manipulowania zawartością.
   7) Proponowane rozwiązanie musi obsługiwać rozłączanie stron internetowych jednym kliknięciem, aby zablokować dostęp w przypadku wykrycia manipulacji.
4. **Ochrona bezpieczeństwa sieci**
   1) Proponowane rozwiązanie musi być w stanie chronić przed atakami typu " denial of service ", w tym atakami Ping of Death, atakami Teardrop, atakami fragmentacji IP, atakami Smerf & Fraggle, atakami typu Land, atakami ICMP dużych pakietów itp.
   2) Obsługa ochrony przed atakami zalewającymi zapytania DNS (flood).
   3) Proponowane rozwiązanie musi być w stanie chronić przed nieprawidłowościami protokołu TCP.
   4) Proponowane rozwiązanie musi być w stanie chronić przed skanowaniem/spoofingiem adresów IP i skanowaniem portów.
   5) Proponowane rozwiązanie musi być w stanie chronić przed atakim typu Flood, w tym ICMP Flood, UDP Flood, SYN Flood itp.
   6) Proponowane rozwiązanie musi obsługiwać bazę danych reputacji IP i blokować złośliwe IP.
   7) Monitorowanie logów poprzez mobilną aplikację dla systemów Android.
   8) Wsparcie dla Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referrer, Cookie do kontroli polityk nagłówków HTTP.
   9) Proponowane rozwiązanie musi obsługiwać HTTP2 w trybie reverse proxy.
   10) Proponowane rozwiązanie musi obsługiwać HTTP2 W trybie non-listening.
   11) Obsługa analizy HTTPS w trybie monitorowania obejścia (bypass) . Obsługa wykrywania ruchu IPv6.
5. **Protokół IPv6**
   1) Proponowane rozwiązanie musi obsługiwać podwójny stos IPv4/IPv6. Adresy IPv4 i IPv6 można dodawać w tym samym czasie co chronione witryny web.
   2) Proponowane rozwiązanie musi obsługiwać wykrywanie i ochronę ruchu dostępowego IPv6.
6. **Strategia samouczenia się**
   1) Proponowane rozwiązanie musi wspierać inteligentne uczenie się ruchu w miejscu ochrony i generować ukierunkowane strategie ochrony w oparciu o wyniki nauczania.
   2) Proponowane rozwiązanie musi być w stanie nauczyć się informacji opartych o obejmujące dynamiczne adresy URL, parametry URL, metody dostępu HTTP, pliki cookie i inne informacje.
   3) Proponowane rozwiązanie musi obsługiwać tryb uczenia się i tryb ochrony. Po nauce może automatycznie przełączyć się w tryb ochrony.
   4) Proponowane rozwiązanie musi obsługiwać, a nie uczyć się dla określonych adresów URL jako wyjątków.
7. **Akcja obronna**

1) Proponowane rozwiązanie musi obsługiwać tylko alarmy w konfiguracji reguł.
2) Proponowane rozwiązanie musi obsługiwać blokowanie i wysyłanie strony alertu dla zachowania, które wyzwala regułę bezpieczeństwa.
3) Proponowane rozwiązanie musi obsługiwać ręczne dostosowywanie strony alertu blokującego.
4) Proponowane rozwiązanie musi obsługiwać przekierowanie strony alertu pod inny adres URL.
5) Proponowane rozwiązanie musi obsługiwać dodawanie białej listy reguł (wyjątek reguły) zgodnie z logami bezpieczeństwa sieci i wyjątkiem reguły zasad.
6) Obsługa wyjątków reguł globalnie lub per site,
7) Obsługa żądań parametrów linii i żądań wyjątków treści na podstawie źródłowego adresu IP, adresu URL, nagłówka http."
8) Proponowane rozwiązanie musi mieć możliwość dodawania intruzów do czarnej listy, aby zablokować późniejszy dostęp.
9) Proponowane rozwiązanie musi obsługiwać białą listę adresów IP i adresów URL.
10) Proponowane rozwiązanie musi obsługiwać powiązanie z zaporą sieciową w celu umieszczenia na czarnej liście.
11) Proponowane rozwiązanie musi obsługiwać kontrolę dostępu w oparciu o GeoIP. Możliwość ograniczenia dostępu do niektórych regionów.
12) Proponowane rozwiązanie musi obsługiwać połączenie z platformą analizy zagrożeń w celu sprawdzenia szczegółów zagrożenia powiązanego adresu IP i plików dla wykrytych zdarzeń zagrożenia.

8. **Tryb wdrażania**
   1) Proponowane rozwiązanie musi obsługiwać przejrzyste wdrożenie in-line bez zmiany konfiguracji sieci.
   2) Proponowane rozwiązanie musi obsługiwać wdrażanie typu tap (mirroing) bez zmiany konfiguracji sieci.
   3) Proponowane rozwiązanie musi obsługiwać wdrażanie w trybie Reverse Proxy.
   4) Proponowane rozwiązanie musi obsługiwać wdrożenie typu Single-Arm.
   5) Proponowane rozwiązanie musi obsługiwać wdrożenie w wykorzystywanie wstrzykiwania Policy Based Routing (przekierowanie routingiem).
   6) Proponowane rozwiązanie musi obsługiwać automatyczne wyszukiwanie, które może wykrywać strony internetowe w sieci i dodawać je jako chronione witryny za pomocą jednego kliknięcia.
   7) Proponowane rozwiązanie musi obsługiwać domyślną witrynę, aby poprawić wydajność korzystania z Internetu.
   8) Proponowane rozwiązanie musi obsługiwać kreatora wdrażania GUI.
   9) Proponowane rozwiązanie musi obsługiwać izolację routingu dla wielu lokalizacji.
9. **Wysoka dostępność**
   1) Proponowane rozwiązanie musi obsługiwać tryb HA-Active/Passive.
   2) Proponowane rozwiązanie musi obsługiwać tryb HA-Active/Active Peer Mode.
   3) Proponowane rozwiązanie musi obsługiwać funkcję bypass poprzez wbudowane lub sieciowe karty sieciowe.
   4) Wszystkie standardowe porty elektryczne usługi w proponowanym rozwiązaniu muszą obsługiwać funkcję obejścia sprzętowego.
   5) Interfejsy rozszerzeń w proponowanym rozwiązaniu muszą obsługiwać wbudowane obejście sprzętowe.
   6) Proponowane rozwiązanie musi obsługiwać konfigurację programowego bypass (w trybie transparentnym). Gdy procesor i liczba równoczesnych połączeń przekroczą próg, można nadać priorytet w celu zapewnienia łączności biznesowej.
10. **Przyspieszanie aplikacji i współdzielenie obciążenia serwera**
    1) Proponowane rozwiązanie musi obsługiwać pamięć podręczną sieci, kompresję stron i usługę połączenia TCP, obsługiwać odciążanie SSL / proxy SSL w celu zmniejszenia presji na serwer WWW.
    2) Proponowane rozwiązanie musi obsługiwać podział obciążenia serwera (w trybie reverse proxy), obsługiwać weighted round robin, least connection i IP Hash algorytm.
    3) Proponowane rozwiązanie musi obsługiwać protokół IPv6 na potrzeby równoważenia obciążenia serwera i transformacji IPv6 witryny internetowej.
    4) Proponowane rozwiązanie musi obsługiwać sprawdzanie kondycji serwera i konfigurowalny obiekt adresu URL, który ma być używany w kontroli kondycji.
    5) Proponowane rozwiązanie musi obsługiwać X-Header jako adres IP równoważenia obciążenia.
    6) Proponowane rozwiązanie musi obsługiwać buforowanie zasobów statycznych dla odpowiadającej zawartości żądania HTTP GET, HEAD, POST i PUT, aby zmniejszyć liczbę interakcji między klientem a serwerem i przyspieszyć szybkość przetwarzania witryny.
11. **Konfiguracja sieci i interfejsu**
    1) Proponowane rozwiązanie musi obsługiwać routing statyczny.
    2) Proponowane rozwiązanie musi obsługiwać zagregowany interfejs.
    3) Proponowane rozwiązanie musi obsługiwać podinterfejs sieci VLAN.
    4) Proponowane rozwiązanie musi obsługiwać multi-vSwitch i virtual-wire.
    5) Proponowane rozwiązanie musi obsługiwać LLDP.

12. **Zarządzanie urządzeniami**
    1) Proponowane rozwiązanie musi obsługiwać wiele metod zarządzania, takich jak HTTP, HTTPS, SSH, Consola itp. oraz obsługiwać konfigurację zaufanych hostów zarządzania.
    2) Proponowane rozwiązanie musi obsługiwać wielopoziomową funkcję autoryzacji zarządzania, obsługiwać predefiniowane role zarządcze, takie jak administrator systemu, operator, audytor itp.
    3) Proponowane rozwiązanie musi obsługiwać uwierzytelnianie administratora, takie jak uwierzytelnianie lokalne, Radius, TACACS+.
    4) Proponowane rozwiązanie musi być w stanie wyświetlić stan pracy, w tym przegląd i szczegółowe informacje o dysku twardym, pamięci, procesorze i wykorzystaniu temperatury.
    5) Proponowane rozwiązanie musi obsługiwać scentralizowane zarządzanie i może wykonywać scentralizowaną aktualizację wielu urządzeń WAF za pośrednictwem scentralizowanego systemu zarządzania.
    6) Proponowane rozwiązanie musi obsługiwać narzędzia hping/tcpdump/curl.
13. **Dzienniki, raporty i alerty**
    1) Proponowane rozwiązanie musi być w stanie zapewnić bogate informacje o rejestrowaniu, w tym logi zarządzania urządzeniami, logi bezpieczeństwa sieci, logi manipulacji, logi kontroli dostępu, logi polityk samouczących się, logi dostępu do sieci itp.
    2) Proponowane rozwiązanie musi obsługiwać rejestrowanie wszystkich zdarzeń ataku nagłówka żądania HTTP, w tym żądanego adresu URL, agenta użytkownika, treści POST, pliku cookie itp.
    3) Proponowane rozwiązanie musi obsługiwać rejestrowanie informacji o odpowiedziach serwera.
    4) Proponowane rozwiązanie musi obsługiwać rejestrowanie komunikatów odpowiedzi w logach zabezpieczeń sieci Web, logach ochrony API i logach naruszeń modelu samouczącego się, aby zapewnić użytkownikom więcej dowodów do analizy zachowań związanych z atakami.
    5) Proponowane rozwiązanie musi obsługiwać wiele metod ostrzegania, takich jak EMAIL, SNMP, SYSLOG, SMS.
    6) Proponowane rozwiązanie musi być w stanie zapewnić wiele szablonów raportów, takich jak przegląd zagrożeń bezpieczeństwa, szczegóły ryzyka witryny, szczegóły typu ataku, analiza manipulacji witryny, wizyty w witrynie, podsumowanie ataku w warstwie sieciowej, stan działania systemu itp.
    7) Proponowane rozwiązanie musi być w stanie zapewnić wielowymiarowe szablony raportów, takie jak przegląd zagrożeń bezpieczeństwa, szczegóły ryzyka witryny, szczegóły typu ataku, wizyty w witrynie, podsumowanie ataku w warstwie sieciowej, stan operacyjny systemu itp.
    8) Proponowane rozwiązanie musi obsługiwać inteligentną analizę logów, która obejmuje analizę zagrożeń i analizę fałszywych alarmów. Na podstawie wyników analizy można przeprowadzić optymalizację polityk bezpieczeństwa jednym kliknięciem w celu poprawy ochrony.
    9) Proponowane rozwiązanie musi obsługiwać odtwarzanie ataków, co może pomóc administratorom w szybkiej analizie i identyfikacji zagrożeń/ataków w sieci.
    10) Proponowane rozwiązanie musi obsługiwać false positive i logi raportów, które administrator podejrzewa o false positive.
    11) Proponowane rozwiązanie musi obsługiwać funkcję usuwania logów bezpieczeństwa sieci.
    12) Proponowane rozwiązanie musi obsługiwać funkcję eksportu logów bezpieczeństwa sieci Web.
    13) Proponowane rozwiązanie musi obsługiwać transfer logów do funkcji FTP (wspierane tylko przez wersję poufną).
    14) Proponowane rozwiązanie musi obsługiwać raporty definiowane przez użytkownika.
    15) Proponowane rozwiązanie musi obsługiwać export raportu w formacie PDF, DOC, html.
    16) Proponowane rozwiązanie musi obsługiwać okresowe generowanie raportów.
    17) Proponowane rozwiązanie musi obsługiwać wysyłanie raportów przez FTP i e-mail.
    18) Proponowane rozwiązanie musi obsługiwać raporty PCI-DSS, które mogą oceniać zgodność miejsc ochrony zgodnie ze specyfikacjami PCI-DSS.
    19) Proponowane rozwiązanie musi obsługiwać konfigurację serwera pocztowego z transmisją szyfrowaną STARTTLS i SSL.
    20) Proponowane rozwiązanie musi obsługiwać strategię śledzenia sesji użytkowników, dodawać nazwę użytkownika, identyfikator sesji i wartość identyfikatora sesji w logach.
    21) Proponowane rozwiązanie musi obsługiwać wykrywanie słabych haseł, w tym konfigurację wykrywania pola hasła, pola nazwy użytkownika i złożoności hasła, obsługa powiązania z politykami śledzenia sesji użytkowników i przegląd zabezpieczeń konta.
    22) Proponowane rozwiązanie musi obsługiwać wyświetlanie kraju i regionu źródła ataku na stronie WAF.
    23) Proponowane rozwiązanie musi obsługiwać kombinację logów bezpieczeństwa stron internetowych generowanych przez wyjątki protokołu HTTP, wyciek informacji oraz wykrywanie reguł ochrony, co może skutecznie zmniejszyć liczbę logów i zmniejszyć odsetek fałszywych alarmów logów.
    24) Proponowane rozwiązanie musi obsługiwać filtrowanie logów dostępu do witryny przez IP / URL, aby zmniejszyć nadmiarowe dzienniki.
14. **Widok pełnego ekranu (dedykowany dashboard pełnoekranowy)**

1) Proponowane rozwiązanie musi obsługiwać przełączanie przez mapę świata, co pozwoli na bardziej dynamiczne i intuicyjne wyświetlanie trendów ataków.
2) Proponowane rozwiązanie musi obsługiwać wyświetlanie wszystkich zagrożeń zidentyfikowanych przez urządzenie.
3) Proponowane rozwiązanie musi obsługiwać wyświetlanie zdarzeń o wysokim priorytecie i najnowszych zdarzeń zagrożenia.
4) Proponowane rozwiązanie musi obsługiwać wyświetlanie rozkładu poziomu zagrożeń terenowych, obsługiwać wyświetlanie całkowitej liczby lokalizacji i miejsc ryzyka.
5) Obsługa wyświetlanie wydajności monitorowanych witryn web.

15. **Obsługa uaktualnień**
    1) Bazę sygnatur można uaktualnić ręcznie lub automatycznie, bez ponownego uruchamiania urządzenia podczas procesu aktualizacji, a oryginalne połączenie sesji może być utrzymywane bez zakłóceń.
16. **Zarządzanie konfiguracją**
    1) Proponowane rozwiązanie musi obsługiwać zarządzanie certyfikatami HTTPS, które może obsługiwać eksport certyfikatów, wyświetlać szczegóły certyfikatu, sprawdzać poprawność.
17. **Gwarancja**
    1) 24-miesięczna gwarancja producenta na dostarczone elementy systemu.
    2) Licencja na wszystkie funkcje bezpieczeństwa oraz wsparcie techniczne producenta na oprogramowanie na okres minimum 24 miesięcy.
    3) Wsparcie techniczne dystrybutora rozwiązań w języku polskim.
18. **Szkolenie**
    1) Wykonawca zapewni szkolenie w zakresie użytkowania i administrowania urządzeniem. Szkolenie musi zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta urządzenia. Szkolenie może odbyć się w formie zdalnej.