Załącznik nr 6 – Opis równoważności

Dostawa urządzeń Network Detection and Response i Web Application Firewall.

1. NDR Server Breach Detection System – Hillstone I-1870

Opis równoważności:

Parametr	Charakterystyka
	• Wysokość 1U do montażu w szafie rack. • Posiadać co najmniej dwa porty USB • Urządzenie musi posiadać dedykowany port do zarządzania • Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE • Musi obsługiwać co najmniej 1T przestrzeni dyskowej. • Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń • Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji. • Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
Usługi sieciowe	• Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta. • Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń • Musi posiadać możliwosc rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
Kontrola aplikacji	• Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp. • Rozwiązanie musi być w stanie zidentyfikować aplikacje

	mobilne typu iOS lub Android. • Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
Wykrywanie zagrożeń	• Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń. • Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6 • Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA • Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. • Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku. • Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS. • Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS. • Rozwiązanie musi mieć opcję przechwytywania pakietów • Rozwiązanie musi umieć wykrywa reverse-shell • Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu • System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
Skanowanie antywirusowe:	• Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.

	• Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP. • Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach • Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
Wykrywanie botnetów C&C:	• Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C. • Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C • Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen. • Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS. • Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA. • Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
Sandbox w chmurze	• Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń • Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy. • Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.

	• Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty • Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików. • Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
Wykrywanie spamu	• Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym • Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości. • Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 • Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
Dodatkowe funkcje ochrony:	• Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. • Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP • Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu. • Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
Inteligentne funkcje bezpieczeństwa:	• Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki. • Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym. • Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp

	• Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania • Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut. • Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów. • Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS • Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji • Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym • Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń. • Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia • Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta • Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd. • Rozwiązanie musi obsługiwać przechwytywanie pakietów online • Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania

	• Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych • Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę • Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.
Widoczność ryzyka/zagrożeń:	• Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego. • Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch. • Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu. • Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. • Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni. • Rozwiązanie musi wspierać wskazanie ścieżki ataku.
Analiza i odpowiedzi na incydenty	• Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury • Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach. • Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.

	• Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania. • Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.
Administracja:	• Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) • Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli • Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło • Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. • Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych • Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny • Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
Logowanie i raportowanie:	• Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP. • Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.

	• Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS. • Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń. • Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje • Wstępnie zdefiniowane zadania raportowania • Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni. • Rozwiązanie musi wspierać restAPI
Gwarancja/dostawa:	• 36 – miesięczną gwarancję producenta na dostarczone elementy systemu • Wsparcie techniczne dystrybutora rozwiązań w języku polskim

2. Hillstone W-Series Web Application Firewall – W320S

Opis równoważności:

Specyfikacja	a. Proponowane rozwiązanie musi obsługiwać przepustowość HTTP 1.2 Gbps b. Proponowane rozwiązanie musi obsługiwać minimum 3500 nowych sesji HTTP c. Proponowane rozwiązanie musi obsługiwać minimum 5500 HTTP Transactions Per Second (TPS) d. Proponowane rozwiązanie musi obsługiwać co najmniej 480 GB pamięci na dysku e. Proponowane rozwiązanie musi obsługiwać co najmniej 4 GB RAM f. Proponowane rozwiązanie musi obsługiwać minimalnie 8 interfejsów sieciowych GE g. Proponowane rozwiązanie musi chronić minimum 16 podłączonych aplikacji Web h. Proponowane rozwiązanie musi zabezpieczać minimum 64 pary IP/PORT i. Proponowane rozwiązanie musi być dostarczone w formie fizycznego applliance o wysokości nie wyższej niż 1U j. Proponowane rozwiązanie musi obsługiwać RESTful API

Ochrona aplikacji internetowych	• Proponowane rozwiązanie musi obsługiwać ochronę przed nieprawidłowościami protokołu HTTP • Proponowane rozwiązanie musi obsługiwać transparentne SSL proxy, które może chronić stronę HTTPS • 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 • Proponowane rozwiązanie musi wspierać ochronę przed atakiem Fast HTTP Flood i powolnym atakiem HTTP Flood • Proponowane rozwiązanie musi obsługiwać HTTP Flooding - ochrona przed atakami Brute Force obejmująca wiele metod, takich jak statystyki użytkowników, kody weryfikacyjne, ograniczanie szybkości itp. • 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. • Proponowane rozwiązanie musi obsługiwać funkcje Cross Site Attack/Defense i może bronić przed atakami XSS i CSRF

	• Proponowane rozwiązanie musi obsługiwać możliwości inteligentnego wykrywania semantycznego dla ataków SQL injection i XSS • Proponowane rozwiązanie musi obsługiwać konfigurację różnej czułości reguły wykrywania wstrzykiwania XSS/SQL w celu ochrony przed różnymi poziomami zagrożeń i poprawy dokładności wykrywania • 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. • Obsługa funkcji zapobiegania wyciekom poufnych informacji. Może 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). • Obsługa możliwości ochrony plików cookie. Może zapobiec złośliwej ingerencji lub porwaniu plików cookie. Obsługuje również podpisy plików cookie i funkcje szyfrowania. • 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. • 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. • Proponowane rozwiązanie musi obsługiwać funkcje ochrony przed lukami w zabezpieczeniach, które są przeznaczone dla serwerów WWW, frameworków internetowych i aplikacji internetowych. • 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. • Proponowane rozwiązanie musi mieć możliwości ochrony przed złośliwym oprogramowaniem i może bronić się przed Web Shell, atakami koni trojańskich itp. • Proponowane rozwiązanie musi mieć zdolność zapobiegania atakom siłowym • 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

	• Proponowane rozwiązanie musi obsługiwać reguły zdefiniowane przez użytkownika • Musi zawierać wstępnie zdefiniowane i niestandardowe szablony polityk zabezpieczeń • Obsługa aktualizacji bazy sygnatur w czasie rzeczywistym • Obsługa funkcji wykrywania i ochrony bezpieczeństwa API. Wsparcie zgodność w oparciu o standardy specyfikacji interfejsu OpenAPI. • Możliwość skonfigurowania stanu strony internetowej jako stanu konserwacji witryny • Proponowane rozwiązanie musi obsługiwać wsadową modyfikację konfiguracji witryny (stan witryny, polityka bezpieczeństwa i alarm, status logów dostępu do sieci web, polityka bezpieczeństwa web) • Proponowane rozwiązanie musi obsługiwać tryb ponownej ochrony, zapewniać odpowiednie kreatory konfiguracji oraz poprawiać wydajność działania i konserwacji bezpieczeństwa podczas ćwiczeń ofensywnych i defensywnych
Wykrywanie manipulacji w sieci web	• Obsługa dwóch trybów pracy: trybu uczenia się i trybu ochrony • Obsługa porównywania chronionych treści na podstawie podobieństwa • Proponowane rozwiązanie musi obsługiwać niestandardową ochronę statycznych stron sieci Web. Możliwość wykluczenia wyjątku listy adresów URL z ochrony przed manipulacją. Obsługa funkcji planowania. • Obsługa wbudowanego silnika synchronizacji w celu synchronizacji zawartości z serwerów internetowych i ustanowienia linii bazowej • Obsługa sabotażu i normalnego monitorowania modyfikacji • Wsparcie kryminalistyki w zakresie manipulowania zawartością • Proponowane rozwiązanie musi obsługiwać rozłączanie stron internetowych jednym kliknięciem, aby zablokować dostęp w przypadku wykrycia manipulacji.
Ochrona bezpieczeństwa sieci	• 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. • Obsługa ochrony przed atakami zalewającymi zapytania DNS (flood), a wartość alertu można ustawić zgodnie ze źródłem i miejscem docelowym • Proponowane rozwiązanie musi być w stanie chronić przed nieprawidłowościami protokołu TCP • Proponowane rozwiązanie musi być w stanie chronić przed skanowaniem/spoofingiem adresów IP i skanowaniem portów • Proponowane rozwiązanie musi być w stanie chronić przed atakim typu Flood, w tym ICMP Flood, UDP Flood, SYN Flood itp.

	• Proponowane rozwiązanie musi obsługiwać bazę danych reputacji IP i blokować złośliwe IP • Monitorowanie logów poprzez mobilną aplikację dla systemów Android, IOS • Wsparcie dla Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referrer, Cookie do kontroli polityk nagłówków HTTP • Proponowane rozwiązanie musi obsługiwać HTTP2 w trybie reverse proxy • Proponowane rozwiązanie musi obsługiwać HTTP2 W trybie non-listening • Obsługa analizy HTTPS w trybie monitorowania obejścia (bypass) . Obsługa wykrywania ruchu IPv6
Protokół IPv6	• Proponowane rozwiązanie musi obsługiwać podwójny stosu IPv4/IPv6. Adresy IPv4 i IPv6 można dodawać w tym samym czasie co chronione witryny web • Proponowane rozwiązanie musi obsługiwać wykrywanie i ochronę ruchu dostępowego IPv6
Strategia samouczenia się	• Proponowane rozwiązanie musi wspierać inteligentne uczenie się ruchu w miejscu ochrony i generować ukierunkowane strategie ochrony w oparciu o wyniki nauczania. • Proponowane rozwiązanie musi być w stanie nauczyć się informacji opartych obejmujące dynamiczne adresy URL, parametry URL, metody dostępu HTTP, pliki cookie i inne informacje • Proponowane rozwiązanie musi obsługiwać tryb uczenia się i tryb ochrony. Po nauce może automatycznie przełączyć się w tryb ochrony. • Proponowane rozwiązanie musi obsługiwać, a nie uczyć się dla określonych adresów URL jako wyjątków.
Akcja obronna	• Proponowane rozwiązanie musi obsługiwać tylko alarmy w konfiguracji reguł • Proponowane rozwiązanie musi obsługiwać blokowanie i wysyłanie strony alertu dla zachowania, które wyzwala regułę bezpieczeństwa • Proponowane rozwiązanie musi obsługiwać ręczne dostosowywanie strony alertu blokującego • Proponowane rozwiązanie musi obsługiwać przekierowanie strony alertu pod inny adres URL • Proponowane rozwiązanie musi obsługiwać dodawanie białej listy reguł (wyjątek reguły) zgodnie z logami bezpieczeństwa sieci i wyjątkiem reguły zasad, • obsługa wyjątków reguł globalnie lub per site, • obsługa żądań parametrów linii i żądań wyjątków treści na podstawie źródłowego adresu IP, adresu URL, nagłówka http." • Proponowane rozwiązanie musi mieć możliwość dodawania intruzów do czarnej listy, aby zablokować późniejszy dostęp

	• Proponowane rozwiązanie musi obsługiwać białą listę adresów IP i adresów URL • Proponowane rozwiązanie musi obsługiwać powiązanie z zaporą sieciową w celu umieszczenia na czarnej liście • Proponowane rozwiązanie musi obsługiwać kontrolę dostępu w oparciu o GeoIP. Możliwość ograniczenia dostępu do niektórych regionów. • Proponowane rozwiązanie musi obsługiwać połączenie z platformą analizy zagrożeń w celu sprawdzenia szczegółów zagrożenia powiązanego adresu IP i plików dla wykrytych zdarzeń zagrożenia
Tryb wdrażania	• Proponowane rozwiązanie musi obsługiwać przejrzyste wdrożenie in-line bez zmiany konfiguracji sieci • Proponowane rozwiązanie musi obsługiwać wdrażanie typu tap (mirroing) bez zmiany konfiguracji sieci • Proponowane rozwiązanie musi obsługiwać wdrażanie w trybie Reverse Proxy • Proponowane rozwiązanie musi obsługiwać wdrożenie typu Single-Arm • Proponowane rozwiązanie musi obsługiwać wdrożenie w wykorzystywanie wstrzykiwanie Policy Based Routing (przekierowanie routingiem) • Proponowane rozwiązanie musi obsługiwać automatyczne wyszukiwanie, które może wykrywać strony internetowe w sieci i dodawać je jako chronione witryny za pomocą jednego kliknięcia • Proponowane rozwiązanie musi obsługiwać domyślną witrynę, aby poprawić wydajność korzystania z Internetu. • Proponowane rozwiązanie musi obsługiwać kreatora wdrażania GUI • Proponowane rozwiązanie musi obsługiwać izolację routingu dla wielu lokalizacji
Wysoka dostępność	• Proponowane rozwiązanie musi obsługiwać tryb HA-Active/Passive • Proponowane rozwiązanie musi obsługiwać tryb HA-Active/Active Peer Mode • Proponowane rozwiązanie musi obsługiwać funkcję bypass poprzez wbudowane lub sieciowe karty sieciowe • Wszystkie standardowe porty elektryczne usługi w proponowanym rozwiązaniu muszą obsługiwać funkcję obejścia sprzętowego • Interfejsy rozszerzeń w proponowanym rozwiązaniu muszą obsługiwać wbudowane obejście sprzętowe • 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

Przyspieszanie aplikacji i współdzielenie obciążenia serwera	• 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. • Proponowane rozwiązanie musi obsługiwać podział obciążenia serwera (w trybie reverse proxy), obsługiwać weighted round robin, least connection i IP Hash algorytm • Proponowane rozwiązanie musi obsługiwać protokół IPv6 na potrzeby równoważenia obciążenia serwera i transformacji IPv6 witryny internetowej • Proponowane rozwiązanie musi obsługiwać sprawdzanie kondycji serwera i konfigurowalny obiekt adresu URL, który ma być używany w kontroli kondycji. • Proponowane rozwiązanie musi obsługiwać X-Header jako adres IP równoważenia obciążenia. • 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
Konfiguracja sieci i interfejsu	• Proponowane rozwiązanie musi obsługiwać routing statyczny • Proponowane rozwiązanie musi obsługiwać zagregowany interfejs • Proponowane rozwiązanie musi obsługiwać podinterfejs sieci VLAN • Proponowane rozwiązanie musi obsługiwać multi-vSwitch i virtual-wire • Proponowane rozwiązanie musi obsługiwać LLDP
Zarządzanie urządzeniami	• Proponowane rozwiązanie musi obsługiwać wiele metod zarządzania, takich jak HTTP, HTTPS, SSH, Konsola itp. oraz obsługiwać konfigurację zaufanych hostów zarządzania. • Proponowane rozwiązanie musi obsługiwać wielopoziomową funkcję autoryzacji zarządzania, obsługiwać predefiniowane role zarządcze, takie jak administrator systemu, operator, audytor itp. • Proponowane rozwiązanie musi obsługiwać uwierzytelnianie administratora, takie jak uwierzytelnianie lokalne, Radius, TACACS+. • Proponowane rozwiązanie musi być w stanie wyświetlić stan pracy, w tym przegląd i szczegółowe informacje o dysku twardym, pamięci, procesorze i wykorzystaniu temperatury. • Proponowane rozwiązanie musi obsługiwać scentralizowane zarządzanie i może wykonywać scentralizowaną aktualizację wielu urządzeń WAF za pośrednictwem scentralizowanego systemu zarządzania. • Proponowane rozwiązanie musi obsługiwać narzędzia hping/tcpdump/curl

Dzienniki, raporty i alerty	• Proponowane rozwiązanie musi być w stanie zapewnić bogate informacje o rejestrowaniu, w tymlogi zarządzania urządzeniami, logi bezpieczeństwa sieci, logi manipulacji, logi kontroli dostępu, logi polityk samouczących się, logi dostępu do sieci itp. • Proponowane rozwiązanie musi obsługiwać rejestrowanie wszystkich zdarzeń ataku nagłówka żądania HTTP, w tym żądanego adresu URL, agenta użytkownika, treści POST, pliku cookie itp. • Proponowane rozwiązanie musi obsługiwać rejestrowanie informacji o odpowiedziach serwera. • 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 • Proponowane rozwiązanie musi obsługiwać wiele metod ostrzegania, takich jak EMAIL, SNMP, SYSLOG, SMS • 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. • 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. • 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. • Proponowane rozwiązanie musi obsługiwać odtwarzanie ataków, co może pomóc administratorom w szybkiej analizie i identyfikacji zagrożeń/ataków w sieci. • Proponowane rozwiązanie musi obsługiwać false positive i logi raportów, które administrator podejrzewa o false positive • Proponowane rozwiązanie musi obsługiwać funkcję usuwania logów bezpieczeństwa sieci • Proponowane rozwiązanie musi obsługiwać funkcję eksportu logów bezpieczeństwa sieci Web • Proponowane rozwiązanie musi obsługiwać transfer logów do funkcji FTP (wspierane tylko przez wersję poufną) • Proponowane rozwiązanie musi obsługiwać raporty definiowane przez użytkownika

	• Proponowane rozwiązanie musi obsługiwać export raportu w formacie PDF, DOC, html • Proponowane rozwiązanie musi obsługiwać okresowe generowanie raportów • Proponowane rozwiązanie musi obsługiwać wysyłanie raportów przez FTP i e-mail • Proponowane rozwiązanie musi obsługiwać raporty PCI-DSS, które mogą oceniać zgodność miejsc ochrony zgodnie ze specyfikacjami PCI-DSS • Proponowane rozwiązanie musi obsługiwać konfigurację serwera pocztowego z transmisją szyfrowaną STARTTLS i SSL • Proponowane rozwiązanie musi obsługiwać strategię śledzenia sesji użytkowników, dodawać nazwę użytkownika, identyfikator sesji i wartość identyfikatora sesji w logach • 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 • Proponowane rozwiązanie musi obsługiwać wyświetlanie kraju i regionu źródła ataku na stronie WAF. • 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 • Proponowane rozwiązanie musi obsługiwać filtrowanie logów dostępu do witryny przez IP / URL, aby zmniejszyć nadmiarowe dzienniki
Widok pełnego ekran (dedykowany dashboard pełnoekranowy)	• Proponowane rozwiązanie musi obsługiwać przełączanie przez mapę świata, co pozwoli na bardziej dynamiczne i intuicyjne wyświetlanie trendów ataków • Proponowane rozwiązanie musi obsługiwać wyświetlanie wszystkich zagrożeń zidentyfikowanych przez urządzenie • Proponowane rozwiązanie musi obsługiwać wyświetlanie zdarzeń o wysokim priorytecie i najnowszych zdarzeń zagrożenia" • Proponowane rozwiązanie musi obsługiwać wyświetlanie rozkładu poziomu zagrożeń terenowych, obsługiwać wyświetlanie całkowitej liczby lokalizacji i miejsc ryzyka, • Obsługa wyświetlanie wydajności monitorowanych witryn web
Obsługa uaktualnień	• Bazę sygnatur można uaktualnić ręcznie lub automatycznie, bez ponownego uruchamiania urządzenia podczas procesu aktualizacji, a oryginalne połączenie sesji może być utrzymywane bez zakłóceń

Zarządzanie konfiguracją	• Proponowane rozwiązanie musi obsługiwać zarządzanie certyfikatami HTTPS, które może obsługiwać eksport certyfikatów, wyświetlać szczegóły certyfikatu, sprawdzać poprawność
Certyfikaty	• ISO 9001:2015, ISO 27001:2013, ISO 45001:2018, ISO 50001:2018, ISO 27701:2019, RoHS, CE, FCC
Gwarancja	• 36-miesięczna gwarancja producenta na dostarczone elementy systemu • Oferowane rozwiązania powinny posiadać aplikację mobilną, dzięki której będą mogły monitorować i analizować swoją pracę