

**Opis przedmiotu zamówienia****Wymagania ogólne(wspólne) w zakresie dostawy:**

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia muszą być zasilane bezpośrednio z sieci 230V.
6. Wszystkie urządzenia muszą pochodzić od jednego producenta i być w pełni kompatybilne ze sobą.

**Urządzenie klasy NDR****– rozwiązanie do wykrywania i reagowania na różnego rodzaju ataki sieciowe i zagrożenia****Minimalne parametry techniczne i funkcjonalne:**

1. **Elementy systemu bezpieczeństwa**
  - 1) Wysokość maks. 1U do montażu w szafie rack(elementy mocujące w zestawie).
  - 2) Posiadać co najmniej dwa porty USB.
  - 3) Urządzenie musi posiadać dedykowany port do zarządzania.
  - 4) Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE.
  - 5) Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
  - 6) Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń.
  - 7) Rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
  - 8) Rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
2. **Usługi sieciowe**
  - 1) Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
  - 2) Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń.
  - 3) Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
3. **Kontrola aplikacji**
  - 1) 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.
  - 2) Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
  - 3) 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.
4. **Wykrywanie zagrożeń**
  - 1) Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
  - 2) Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6.
  - 3) Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
  - 4) Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
  - 5) Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
  - 6) Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
  - 7) Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
  - 8) Rozwiązanie musi mieć opcję przechwytywania pakietów.

- 9) Rozwiązanie musi umieć wykrywać reverse-shell.
- 10) Rozwiązanie musi potrafić zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu.
- 11) System musi mapować wykryte zagrożenia na framework MITRE ATT&CK.
5. **Skanowanie antywirusowe**
  - 1) Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
  - 2) Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
  - 3) 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.
  - 4) Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików.
6. **Wykrywanie botnetów C&C**
  - 1) Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
  - 2) Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C.
  - 3) Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
  - 4) Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
  - 5) Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
  - 6) Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS, a także rejestrować logów zagrożeń wykrytych tuneli DNS.
7. **Sandbox w chmurze**
  - 1) Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanymi zagrożeń.
  - 2) Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
  - 3) Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
  - 4) Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF oraz skrypty.
  - 5) Rozwiązanie powinno dostarczać kompletny raport analizy behawioralnej dla złośliwych plików.
  - 6) Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznanne zagrożenie.
8. **Wykrywanie spamu**
  - 1) Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym.
  - 2) Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
  - 3) Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3.
  - 4) Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
9. **Dodatkowe funkcje ochrony**
  - 1) Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
  - 2) Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP.
  - 3) Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
  - 4) Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp.
10. **Inteligentne funkcje bezpieczeństwa**
  - 1) Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
  - 2) Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
  - 3) Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanymi rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp.
  - 4) Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania.
  - 5) Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
  - 6) 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.

- 7) Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DdoS.
  - 8) Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji.
  - 9) Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym.
  - 10) Rozwiązanie musi zapewniać analizę kryminalistyczną, w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
  - 11) Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia.
  - 12) Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta.
  - 13) Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
  - 14) Rozwiązanie musi obsługiwać przechwytywanie pakietów online.
  - 15) Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania.
  - 16) Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych.
  - 17) Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę.
  - 18) Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekho, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalności funkcji śledzenia zagrożeń.
11. **Widoczność ryzyka/zagrożeń**
- 1) Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
  - 2) Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
  - 3) Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na goście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
  - 4) Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
  - 5) Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
  - 6) Rozwiązanie musi wspierać wskazanie ścieżki ataku.
12. **Analiza i odpowiedzi na incydenty**
- 1) Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury.
  - 2) Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
  - 3) Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
  - 4) Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
  - 5) 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 odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail).
13. **Administracja**
- 1) Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI).
  - 2) Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli.
  - 3) Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło.
  - 4) Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
  - 5) Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych.
  - 6) Rozwiązanie powinno posiadać aplikację mobilną pozwalającą na monitoring pracy i analizę zdarzeń.
14. **Logowanie i raportowanie**
- 1) Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
  - 2) Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
  - 3) Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.

- 4) Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
  - 5) Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje.
  - 6) Rozwiązanie powinno posiadać wstępnie zdefiniowane zadania raportowania.
  - 7) 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.
  - 8) Rozwiązanie musi wspierać restAPI.
15. **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.
16. **Szkolenie**
- 1) Z wdrożonego rozwiązania musi zostać przeprowadzone szkolenie w zakresie użytkowania i administrowania nim.
  - 2) Szkolenie musi zostać przeprowadzone w języku polskim – do szkolenia muszą być zapewnione materiały szkoleniowe.
  - 3) Szkolenie musi zostać przeprowadzone przez osoby posiadające należyte doświadczenie i odpowiednią wiedzę merytoryczną w zakresie objętym tematyką szkolenia.
  - 4) Szkolenie musi zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającym wspomniane umiejętności.
  - 5) Szkolenie może odbyć się w formie zdalnej.

**Urządzenie klasy IPS**  
**– rozwiązanie do zapobiegania włamaniom**

**Minimalne parametry techniczne i funkcjonalne:**

1. **Elementy systemu bezpieczeństwa**
  - 1) Maksymalna wysokość 1U(elementy mocujące w zestawie).
  - 2) Rozwiązanie musi posiadać co najmniej dwa porty USB.
  - 3) Rozwiązanie musi posiadać co najmniej jeden port konsoli.
  - 4) Rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem.
  - 5) Rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet.
  - 6) Rozwiązanie musi posiadać co najmniej 8 stałych portów SFP.
  - 7) Rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+.
  - 8) Rozwiązanie musi posiadać co najmniej 480GB przestrzeni dyskowej.
  - 9) Rozwiązanie musi obsługiwać przepustowość IPS 3 Gb/s.
  - 10) Rozwiązanie musi obsługiwać jednoczesne sesje o długości 1.2 M.
  - 11) Rozwiązanie musi obsługiwać min 40000 nowych sesji/sekundę w ruchu TCP.
  - 12) Opóźnienia (tzw. Latency) nie mogą przekraczać 300µs.
  - 13) Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW.
2. **Usługi sieciowe**
  - 1) Rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu).
3. **Kontrola Aplikacji**
  - 1) Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów, czasu online, czasu offline.
  - 2) Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka.
  - 3) Rozwiązanie powinno rozpoznawać aplikacje IPv6.
  - 4) Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL.
  - 5) Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS.
  - 6) Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie ruchu dla aplikacji.
  - 7) Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze.
4. **Ochrona przez zagrożeniami**
  - 1) Rozwiązanie musi obsługiwać ponad 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń.
  - 2) Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL.
  - 3) Rozwiązanie musi obsługiwać ochronę środowiska IPV6.
  - 4) Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS.
  - 5) Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych.



- 6) Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA.
- 7) Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu.
- 8) Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia.
- 9) Rozwiązanie musi obsługiwać opcję logowania pakietów.
- 10) Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu.
- 11) Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp.
- 12) Rozwiązanie musi wspierać weryfikację protokołów http typu Get, Head, Put, Post.
- 13) Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS.
- 14) Rozwiązanie musi obsługiwać tryb działania sniffera IDS.
- 15) Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS.
- 16) Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS.
- 17) Rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP.
- 18) Rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS.
- 19) Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6.
- 20) Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków.
- 21) Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet.
- 22) Obsługa inspekcji Reverse Shell.
- 23) Ochrona i wykrywanie skanowania protokołów IP oraz UDP.
- 24) Rozwiązanie musi mieć możliwość inspekcji payloadu w ramach MPLS.
- 25) Rozwiązanie musi pozwalać na automatyczne określanie wartości proponowanych dla ochrony przed atakami Flood.
- 26) System musi pozwalać na zdefiniowanie globalnej białej listy, pozwalając na dany ruch i nie sprawdzając go na warstwie aplikacyjnej.
- 27) System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK.
5. **Monitoring**
  - 1) Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym nazwę ataku, ważność, czasem, adresem, protokołem, zalecanym rozwiązaniem itp.
  - 2) Rozwiązanie musi obsługiwać usługę Threat Intelligence Pushing Service.
  - 3) Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym.
  - 4) Rozwiązanie powinno obsługiwać monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania itp.
6. **Polityki bezpieczeństwa**
  - 1) Rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS w jednej regule polityki.
  - 2) Rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty.
  - 3) Rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI.
  - 4) Rozwiązanie musi obsługiwać import i eksport polityk.
7. **Administrowanie, logi i raportowanie**
  - 1) Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI).
  - 2) Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę.
  - 3) Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS.
  - 4) Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog.
  - 5) Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora.
  - 6) Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło.
  - 7) Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
  - 8) Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP.
  - 9) Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych.
  - 10) Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania
  - 11) Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i

- alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu.
- 12) Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety.
  - 13) Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi.
  - 14) Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP.
  - 15) Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas.
  - 16) Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania.
  - 17) Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export.
  - 18) Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów.
  - 19) Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog.
  - 20) Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach.
  - 21) Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195).
  - 22) Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika.
  - 23) Rozwiązanie musi obsługiwać zaplanowany raport.
  - 24) Raport powinno być można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP.
  - 25) Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF.
8. **Wysoka dostępność**
- 1) Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive.
  - 2) Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:
    1. HA z agregacją linków
    2. Full mesh HA
    3. Geograficznie rozproszony HA
  - 3) Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA.
9. **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.
10. **Szkolenie**
- 1) Z wdrożonego rozwiązania musi zostać przeprowadzone szkolenie w zakresie użytkowania i administrowania nim.
  - 2) Szkolenie musi zostać przeprowadzone w języku polskim – do szkolenia muszą być zapewnione materiały szkoleniowe.
  - 3) Szkolenie musi zostać przeprowadzone przez osoby posiadające należyte doświadczenie i odpowiednią wiedzę merytoryczną w zakresie objętym tematyką szkolenia.
  - 4) Szkolenie musi zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającym wspomniane umiejętności.
  - 5) Szkolenie może odbyć się w formie zdalnej.

#### Urządzenie klasy WAF

– rozwiązanie do zabezpieczenia serwerów internetowych, aplikacji i interfejsów API

#### Minimalne parametry techniczne i funkcjonalne:

##### 11. Specyfikacja

- 1) Maksymalna wysokość 1U(elementy mocujące w zestawie).
- 2) Rozwiązanie musi obsługiwać przepustowość HTTP 0.6 Gbps
- 3) Rozwiązanie musi obsługiwać minimum 1600 nowych sesji HTTP
- 4) Rozwiązanie musi obsługiwać minimum 2400 HTTP Transactions Per Second (TPS)
- 5) 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) Rozwiązanie musi chronić minimum 8 podłączonych aplikacji Web.

12) Rozwiązanie musi zabezpieczać minimum 64 pary IP/PORT.

13) Rozwiązanie musi obsługiwać RESTful API.

## 12. Ochrona aplikacji internetowych

1) Rozwiązanie musi obsługiwać ochronę przed nieprawidłowościami protokołu HTTP.

2) Rozwiązanie musi obsługiwać transparentne SSL proxy, które może chronić stronę HTTPS.

3) 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) Rozwiązanie musi wspierać ochronę przed atakiem Fast HTTP Flood i powolnym atakiem HTTP Flood.

5) Rozwiązanie musi obsługiwać HTTP Flooding - ochrona przed atakami Brute Force obejmująca wiele metod, takich jak statystyki użytkowników, kody weryfikacyjne, ograniczanie szybkości itp.

6) 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) Rozwiązanie musi obsługiwać funkcje Cross Site Attack/Defense i może bronić przed atakami XSS i CSRF.

8) Rozwiązanie musi obsługiwać możliwości inteligentnego wykrywania semantycznego dla ataków SQL injection i XSS.

9) 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 wyciekowi 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 wyciekowi 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) 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) Rozwiązanie musi obsługiwać funkcje ochrony przed lukami w zabezpieczeniach, które są przeznaczone dla serwerów WWW, frameworków internetowych i aplikacji internetowych.

16) 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) Rozwiązanie musi mieć możliwości ochrony przed złośliwym oprogramowaniem i może bronić się przed Web Shell, atakami koni trojańskich itp.

18) Rozwiązanie musi mieć zdolność zapobiegania atakom siłowym.

19) 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) 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) Rozwiązanie musi obsługiwać wsadową modyfikację konfiguracji witryny (stan witryny, polityka bezpieczeństwa i alarm, status logów dostępu do sieci web, polityka bezpieczeństwa web).

26) Rozwiązanie musi obsługiwać tryb ponownej ochrony, zapewniać odpowiednie kreatory konfiguracji oraz poprawiać wydajność działania i konserwacji bezpieczeństwa podczas ćwiczeń ofensywnych i defensywnych.

## 13. 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) 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) Rozwiązanie musi obsługiwać rozłączanie stron internetowych jednym kliknięciem, aby zablokować dostęp w przypadku wykrycia manipulacji.

#### 14. Ochrona bezpieczeństwa sieci

- 1) 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 & Fraggles, atakami typu Land, atakami ICMP dużych pakietów itp.
- 2) Obsługa ochrony przed atakami zalewającymi zapytania DNS (flood).
- 3) Rozwiązanie musi być w stanie chronić przed nieprawidłowościami protokołu TCP.
- 4) Rozwiązanie musi być w stanie chronić przed skanowaniem/spoofingiem adresów IP i skanowaniem portów.
- 5) Rozwiązanie musi być w stanie chronić przed atakiem typu Flood, w tym ICMP Flood, UDP Flood, SYN Flood itp.
- 6) 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) Rozwiązanie musi obsługiwać HTTP2 w trybie reverse proxy.
- 10) Rozwiązanie musi obsługiwać HTTP2 w trybie non-listening.
- 11) Obsługa analizy HTTPS w trybie monitorowania obejścia (bypass). Obsługa wykrywania ruchu IPv6.

#### 15. Protokół IPv6

- 1) Rozwiązanie musi obsługiwać podwójny stos IPv4/IPv6. Adresy IPv4 i IPv6 można dodawać w tym samym czasie co chronione witryny web.
- 2) Rozwiązanie musi obsługiwać wykrywanie i ochronę ruchu dostępowego IPv6.

#### 16. Strategia samouczenia się

- 1) Rozwiązanie musi wspierać inteligentne uczenie się ruchu w miejscu ochrony i generować ukierunkowane strategie ochrony w oparciu o wyniki nauczania.
- 2) 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) Rozwiązanie musi obsługiwać tryb uczenia się i tryb ochrony. Po nauce może automatycznie przełączyć się w tryb ochrony.
- 4) Rozwiązanie musi obsługiwać, a nie uczyć się dla określonych adresów URL jako wyjątków.

#### 17. Akcja obronna

- 1) Rozwiązanie musi obsługiwać tylko alarmy w konfiguracji reguł.
- 2) Rozwiązanie musi obsługiwać blokowanie i wysyłanie strony alertu dla zachowania, które wyzwala regułę bezpieczeństwa.
- 3) Rozwiązanie musi obsługiwać ręczne dostosowywanie strony alertu blokującego.
- 4) Rozwiązanie musi obsługiwać przekierowanie strony alertu pod inny adres URL.
- 5) 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) Rozwiązanie musi mieć możliwość dodawania intruzów do czarnej listy, aby zablokować późniejszy dostęp.
- 9) Rozwiązanie musi obsługiwać białą listę adresów IP i adresów URL.
- 10) Rozwiązanie musi obsługiwać powiązanie z zaporą sieciową w celu umieszczenia na czarnej liście.
- 11) Rozwiązanie musi obsługiwać kontrolę dostępu w oparciu o GeoIP. Możliwość ograniczenia dostępu do niektórych regionów.
- 12) Rozwiązanie musi obsługiwać połączenie z platformą analizy zagrożeń w celu sprawdzenia szczegółów zagrożenia powiązanego adresu IP i plików dla wykrytych zdarzeń zagrożenia.

#### 18. Tryb wdrażania

- 1) Rozwiązanie musi obsługiwać przejrzyste wdrożenie in-line bez zmiany konfiguracji sieci.
- 2) Rozwiązanie musi obsługiwać wdrażanie typu tap (mirroring) bez zmiany konfiguracji sieci.
- 3) Rozwiązanie musi obsługiwać wdrażanie w trybie Reverse Proxy.
- 4) Rozwiązanie musi obsługiwać wdrożenie typu Single-Arm.
- 5) Rozwiązanie musi obsługiwać wdrożenie w wykorzystywaniu wstrzykiwania Policy Based Routing (przekierowanie routingu).



- 6) Rozwiązanie musi obsługiwać automatyczne wyszukiwanie, które może wykrywać strony internetowe w sieci i dodawać je jako chronione witryny za pomocą jednego kliknięcia.
  - 7) Rozwiązanie musi obsługiwać domyślną witrynę, aby poprawić wydajność korzystania z Internetu.
  - 8) Rozwiązanie musi obsługiwać kreatora wdrażania GUI.
  - 9) Rozwiązanie musi obsługiwać izolację routingu dla wielu lokalizacji.
19. **Wysoka dostępność**
- 1) Rozwiązanie musi obsługiwać tryb HA-Active/Passive.
  - 2) Rozwiązanie musi obsługiwać tryb HA-Active/Active Peer Mode.
  - 3) 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) 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.
20. **Przyspieszanie aplikacji i współdzielenie obciążenia serwera**
- 1) 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) Rozwiązanie musi obsługiwać podział obciążenia serwera (w trybie reverse proxy), obsługiwać weighted round robin, least connection i IP Hash algorytm.
  - 3) Rozwiązanie musi obsługiwać protokół IPv6 na potrzeby równoważenia obciążenia serwera i transformacji IPv6 witryny internetowej.
  - 4) Rozwiązanie musi obsługiwać sprawdzanie kondycji serwera i konfigurowalny obiekt adresu URL, który ma być używany w kontroli kondycji.
  - 5) Rozwiązanie musi obsługiwać X-Header jako adres IP równoważenia obciążenia.
  - 6) 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.
21. **Konfiguracja sieci i interfejsu**
- 1) Rozwiązanie musi obsługiwać routing statyczny.
  - 2) Rozwiązanie musi obsługiwać zagregowany interfejs.
  - 3) Rozwiązanie musi obsługiwać podinterfejs sieci VLAN.
  - 4) Rozwiązanie musi obsługiwać multi-vSwitch i virtual-wire.
  - 5) Rozwiązanie musi obsługiwać LLDP.
22. **Zarządzanie urządzeniami**
- 1) Rozwiązanie musi obsługiwać wiele metod zarządzania, takich jak HTTP, HTTPS, SSH, Consola itp. oraz obsługiwać konfigurację zaufanych hostów zarządzania.
  - 2) Rozwiązanie musi obsługiwać wielopoziomową funkcję autoryzacji zarządzania, obsługiwać predefiniowane role zarządcze, takie jak administrator systemu, operator, audytor itp.
  - 3) Rozwiązanie musi obsługiwać uwierzytelnianie administratora, takie jak uwierzytelnianie lokalne, Radius, TACACS+.
  - 4) Rozwiązanie musi być w stanie wyświetlić stan pracy, w tym przegląd i szczegółowe informacje o dysku twardym, pamięci, procesorze i wykorzystaniu temperatury.
  - 5) Rozwiązanie musi obsługiwać scentralizowane zarządzanie i może wykonywać scentralizowaną aktualizację wielu urządzeń WAF za pośrednictwem scentralizowanego systemu zarządzania.
  - 6) Rozwiązanie musi obsługiwać narzędzia hping/tcpdump/curl.
23. **Dzienniki, raporty i alerty**
- 1) 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) Rozwiązanie musi obsługiwać rejestrowanie wszystkich zdarzeń ataku nagłówka żądania HTTP, w tym żadanego adresu URL, agenta użytkownika, treści POST, pliku cookie itp.
  - 3) Rozwiązanie musi obsługiwać rejestrowanie informacji o odpowiedziach serwera.
  - 4) 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) Rozwiązanie musi obsługiwać wiele metod ostrzegania, takich jak EMAIL, SNMP, SYSLOG, SMS.
  - 6) 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) 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) 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) Rozwiązanie musi obsługiwać odtwarzanie ataków, co może pomóc administratorom w szybkiej analizie i identyfikacji zagrożeń/ataków w sieci.
  - 10) Rozwiązanie musi obsługiwać false positive i logi raportów, które administrator podejrzewa o false positive.
  - 11) Rozwiązanie musi obsługiwać funkcję usuwania logów bezpieczeństwa sieci.
  - 12) Rozwiązanie musi obsługiwać funkcję eksportu logów bezpieczeństwa sieci Web.
  - 13) Rozwiązanie musi obsługiwać transfer logów do funkcji FTP (wspierane tylko przez wersję poufną).
  - 14) Rozwiązanie musi obsługiwać raporty definiowane przez użytkownika.
  - 15) Rozwiązanie musi obsługiwać export raportu w formacie PDF, DOC, html.
  - 16) Rozwiązanie musi obsługiwać okresowe generowanie raportów.
  - 17) Rozwiązanie musi obsługiwać wysyłanie raportów przez FTP i e-mail.
  - 18) Rozwiązanie musi obsługiwać raporty PCI-DSS, które mogą oceniać zgodność miejsc ochrony zgodnie ze specyfikacjami PCI-DSS.
  - 19) Rozwiązanie musi obsługiwać konfigurację serwera pocztowego z transmisją szyfrowaną STARTTLS i SSL.
  - 20) Rozwiązanie musi obsługiwać strategię śledzenia sesji użytkowników, dodawać nazwę użytkownika, identyfikator sesji i wartość identyfikatora sesji w logach.
  - 21) 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) Rozwiązanie musi obsługiwać wyświetlanie kraju i regionu źródła ataku na stronie WAF.
  - 23) 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) Rozwiązanie musi obsługiwać filtrowanie logów dostępu do witryny przez IP / URL, aby zmniejszyć nadmiarowe dzienniki.
- 24. Widok pełnego ekranu (dedykowany dashboard pełnoekranowy)**
- 1) Rozwiązanie musi obsługiwać przełączanie przez mapę świata, co pozwoli na bardziej dynamiczne i intuicyjne wyświetlanie trendów ataków.
  - 2) Rozwiązanie musi obsługiwać wyświetlanie wszystkich zagrożeń zidentyfikowanych przez urządzenie.
  - 3) Rozwiązanie musi obsługiwać wyświetlanie zdarzeń o wysokim priorytecie i najnowszych zdarzeń zagrożenia.
  - 4) Rozwiązanie musi obsługiwać wyświetlanie rozkładu poziomego zagrożeń terenowych, obsługiwać wyświetlanie całkowitej liczby lokalizacji i miejsc ryzyka.
  - 5) Obsługa wyświetlania wydajności monitorowanych witryn web.
- 25. 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.
- 26. Zarządzanie konfiguracją**
- 1) Rozwiązanie musi obsługiwać zarządzanie certyfikatami HTTPS, które może obsługiwać eksport certyfikatów, wyświetlać szczegóły certyfikatu, sprawdzać poprawność.
- 27. 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.
- 28. Szkolenie**
- 1) Z wdrożonego rozwiązania musi zostać przeprowadzone szkolenie w zakresie użytkowania i administrowania nim.
  - 2) Szkolenie musi zostać przeprowadzone w języku polskim – do szkolenia muszą być zapewnione materiały szkoleniowe.
  - 3) Szkolenie musi zostać przeprowadzone przez osoby posiadające należyte doświadczenie i odpowiednią wiedzę merytoryczną w zakresie objętym tematyką szkolenia.
  - 4) Szkolenie musi zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającym wspomniane umiejętności.
  - 5) Szkolenie może odbyć się w formie zdalnej.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA