Załącznik Nr 3

Urządzenie klasy IPS – rozwiązanie do zapobiegania włamaniom

Opis przedmiotu szacowania:

Minimalne parametry techniczne i funkcjonalne:

1. **Elementy systemu bezpieczeństwa**
   1) Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U(elementy mocujące w zestawie).
   2) Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB.
   3) Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli.
   4) Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem.
   5) Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet.
   6) Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP.
   7) Proponowane rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+.
   8) Proponowane rozwiązanie musi posiadać co najmniej 480GB przestrzeni dyskowej.
   9) Proponowane rozwiązanie musi obsługiwać przepustowość IPS 3 Gb/s.
   10) Proponowane rozwiązanie musi obsługiwać jednoczesne sesje o długości 1.2 M.
   11) Proponowane rozwiązanie musi obsługiwać min 40000 nowych sesji/sekundę w ruchu TCP.
   12) Opóźnienia (tzw. Latency) nie mogę przekraczać 300µs.
   13) Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW.
2. **Usługi sieciowe**
   1) Proponowane 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) Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP.
   18) Proponowane 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 payloudu w ramkach 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) Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS w jednej regule polityki.
   2) Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty.
   3) Proponowane 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:
      a) HA z agregacją linków
      b) Full mesh HA
      c) 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) 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.