OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup usług serwisowych oraz subskrypcji dla urządzeń firmy Palo Alto Networks na okres 36 miesięcy

1. Przedmiotem zamówienia jest zakup usług serwisowych oraz subskrypcji dla urządzeń firmy Palo Alto Networks zaimplementowanych w infrastrukturze zamawiającego.
2. W ramach zamówienia Wykonawca zapewni asystę techniczną do etapu poprawnego powiązania subskrypcji będących przedmiotem zamówienia na wskazanych urządzeniach zamawiającego
3. Wsparcie producenta rozwiązania należy zapewnić na okres 36 miesięcy od dnia zawarcia umowy i musi ono obejmować:
    - diagnostykę zdarzeń dotyczących oprogramowania;
    - dostarczanie rozwiązań błędów oprogramowania;
    - zapewnienie łat (ang. patches), tj. poprawek lub aktualizacji mających na celu usunięcie problemów, błędów, rozszerzenie funkcjonalności lub zwiększenie wydajności wcześniejszej wersji oprogramowania;
    - zapewnienie aktualizacji do nowych, wyższych wersji oprogramowania (ang. upgrades);
    - udzielanie odpowiedzi na zapytania związane z instalacją i eksploatacją dostarczonego oprogramowania;
    - aktualizacje bazy aplikacji;
    - procedurę wymiany sprzętu na nowy w przypadku awarii (RMA)
4. Subskrypcje dla urządzeń **typu pierwszego** muszą obejmować minimum:
    a. Aktualizacje baz sygnatur IPS,
    b. Aktualizacje baz sygnatur AV,
    c. Aktualizacje baz sygnatur AntiSpyware,
    d. Aktualizacje baz dla podstawowej ochrony DNS,
    e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
    f. Analizę zagrożeń typu 0-day w systememie Sandbox,
    g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),
    h. Kontrolę tuneli client-to-site w oparciu o analizę stanu hosta (profilowanie stanu hosta) w ramach systemów operacyjnych Windows, MacOS, Android, Linux, iOS,
    i. Zaawansowaną ochronę DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:
        - wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 30 milionów wpisów.
        - możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

- wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
- wykrywanie domen dynamicznych Dynamic DNS
- wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
- domen fast flux.

5. Subskrypcje dla urządzeń **typu drugiego** muszą obejmować minimum:
    a. Aktualizacje baz sygnatur IPS,
    b. Aktualizacje baz sygnatur AV,
    c. Aktualizacje baz sygnatur AntiSpyware,
    d. Aktualizacje baz dla podstawowej ochrony DNS,
    e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
    f. Analizę zagrożeń typu 0-day w systememie Sandbox,
    g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),
    h. Kontrolę tuneli client-to-site w oparciu o analizę stanu hosta (profilowanie stanu hosta) w ramach systemów operacyjnych Windows, MacOS, Android, Linux, iOS,
    i. Zaawansowaną ochronę DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:
        - wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 30 milionów wpisów.
        - możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
        - wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
        - wykrywanie domen dynamicznych Dynamic DNS
        - wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
        - domen fast flux.
6. Subskrypcje dla urządzeń **typu trzeciego** muszą obejmować minimum:
    a. Aktualizacje baz sygnatur IPS,
    b. Aktualizacje baz sygnatur AV,
    c. Aktualizacje baz sygnatur AntiSpyware,
    d. Aktualizacje baz dla podstawowej ochrony DNS,
    e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
    f. Analizę zagrożeń typu 0-day w systememie Sandbox,
    g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),
7. Subskrypcja dla Systemu Centralnego Zarządzania urządzeniami NGFW.

Zamawiający posiada w swojej infrastrukturze system do Centralnego Zarządzania firewallami o nazwie Palo Alto Networks Panorama, który zarządza posiadanymi klastrami urządzeń PA-5220 oraz PA-3220 Zamawiający wymaga, aby w ramach oferty uwzględnić zakup usługi wsparcia na system Centralnego Zarządzania Panorama. Oferta wsparcia dla Systemu Centralnego Zarządzania należy zapewnić na okres 36 miesięcy, w oparciu o usługę określaną jako wsparcie partnerskie, opisaną kodem producenta jako

PAN-SVC-BKLN-PRA-25-3YR-R – Partner enabled premium support 3 year term renewal, Panorama 25 devices

8. Zestawienie modeli wraz z numerami seryjnymi oraz wymaganymi w zamówieniu serwisami i subskrypcjami prezentuje tabela:

<table>
<tr><td colspan="3">Klaster urządzeń PA-5220 – urządzenia typu pierwszego</td></tr>
<tr><td>Numer seryjny urządzenia</td><td>013201022788</td><td>013201022724</td></tr>
<tr><td rowspan="7">Wymagane wparcie i subskrypcje w postaci numerów produktowych/ PN</td><td>PAN-PA-5220-TP-3YR-HA2-R</td><td>PAN-PA-5220-TP-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-WF-3YR-HA2-R</td><td>PAN-PA-5220-WF-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-ADVURL-3YR-HA2-R</td><td>PAN-PA-5220-ADVURL-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-GP-3YR-HA2</td><td>PAN-PA-5220-GP-3YR-HA2</td></tr>
<tr><td>PAN-PA-5220-DNS-3YR-HA2</td><td>PAN-PA-5220-DNS-3YR-HA2</td></tr>
<tr><td>PAN-SVC-BKLN-5220-3YR-R</td><td>PAN-SVC-BKLN-5220-3YR-R</td></tr>
<tr><td colspan="3">Klaster urządzeń PA-5220 – urządzenia typu drugiego</td></tr>
<tr><td>Numer seryjny urządzenia</td><td>013201025627</td><td>013201025647</td></tr>
<tr><td rowspan="7">Wymagane wparcie i subskrypcje w postaci numerów produktowych/ PN</td><td>PAN-PA-5220-TP-3YR-HA2-R</td><td>PAN-PA-5220-TP-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-WF-3YR-HA2</td><td>PAN-PA-5220-WF-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-ADVURL-3YR-HA2-R</td><td>PAN-PA-5220-ADVURL-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-5220-GP-3YR-HA2</td><td>PAN-PA-5220-GP-3YR-HA2</td></tr>
<tr><td>PAN-PA-5220-DNS-3YR-HA2-R</td><td>PAN-PA-5220-DNS-3YR-HA2-R</td></tr>
<tr><td>PAN-SVC-BKLN-5220-3YR-R</td><td>PAN-SVC-BKLN-5220-3YR-R</td></tr>
<tr><td colspan="3">Klaster urządzeń PA-3220 – urządzenia typu trzeciego</td></tr>
<tr><td>Numer seryjny urządzenia</td><td>016201024151</td><td>016201024154</td></tr>
<tr><td rowspan="4">Wymagane wparcie i subskrypcje w postaci numerów produktowych/ PN</td><td>PAN-PA-3220-TP-3YR-HA2-R</td><td>PAN-PA-3220-TP-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-3220-WF-3YR-HA2-R</td><td>PAN-PA-3220-WF-3YR-HA2-R</td></tr>
<tr><td>PAN-PA-3220-ADVURL-3YR-HA2-R</td><td>PAN-PA-3220-ADVURL-3YR-HA2-R</td></tr>
<tr><td>PAN-SVC-BKLN-3220-3YR-R</td><td>PAN-SVC-BKLN-3220-3YR-R</td></tr>
<tr><td colspan="3">System Centralnego Zarządzania Panorama</td></tr>
<tr><td>Wymagane wparcie i subskrypcje w postaci numerów produktowych/ PN</td><td colspan="2">PAN-SVC-BKLN-PRA-25-3YR-R – system centralnego zarządzania winien umożliwiać zarządzanie oraz kolekcję logów z minimum 25 urządzeń fizycznych</td></tr>
</table>