Załącznik nr 1 do **Rozdziału III SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA

Odnowienie subskrypcji oprogramowania do centralnego logowania, raportowania i korelacji zdarzeń bezpieczeństwa

I. Postanowienia ogólne

1. Przedmiot zamówienia

Przedmiotem zamówienia jest odnowienie (przedłużenie) subskrypcji oprogramowania eksploatowanego w infrastrukturze Zamawiającego, z zachowaniem ciągłości wsparcia producenta, tj. oprogramowanie do centralnego logowania, raportowania i korelacji zdarzeń z posiadanego systemu zabezpieczeń (firewall UTM).

2. Charakter zamówienia i uzasadnienie użycia nazw własnych

Zamówienie ma charakter kontynuacyjny: dotyczy przedłużenia praw do korzystania z oprogramowania, które Zamawiający posiada, ma wdrożone i eksploatuje. Z tego względu w opisie przedmiotu zamówienia wskazano nazwy handlowe posiadanego oprogramowania – Zamawiający nie jest w stanie opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób bez ich użycia (art. 99 ust. 5 ustawy Pzp). Wskazaniu każdej nazwy towarzyszy dopuszczenie rozwiązań równoważnych, a kryteria oceny równoważności określono w rozdziale II (art. 99 ust. 6 ustawy Pzp).

Numery katalogowe (SKU) podane w niniejszym dokumencie mają charakter wyłącznie informacyjny i służą identyfikacji posiadanych produktów. Identyfikatory licencji, numery seryjne oraz dane kont w portalach producentów zostaną przekazane wybranemu Wykonawcy po zawarciu umowy. Wykonawca może zaoferować inny numer katalogowy tego samego producenta, jeżeli obejmuje on zakres funkcjonalny, liczbę instancji/pojemność i poziom wsparcia nie gorszy niż opisany.

3. Zasady oferowania rozwiązań równoważnych

Zamawiający dopuszcza dwa równorzędne warianty realizacji:

- Wariant A – odnowienie posiadanej subskrypcji: dostarczenie kluczy/kontraktów przedłużających prawo do korzystania z posiadanego oprogramowania i wsparcia producenta na okres wskazany w OPZ, bez przerwy w stosunku do daty wygaśnięcia obecnej subskrypcji.
- Wariant B – rozwiązanie równoważne: dostarczenie kompletnego, nowego systemu innego producenta (lub innego produktu tego samego producenta), który spełnia wszystkie kryteria równoważności wskazane dla danej części, wraz z wdrożeniem, migracją i szkoleniem opisanymi w OPZ, na koszt i ryzyko Wykonawcy, w cenie oferty.

Rozwiązanie równoważne nie musi być tożsame z rozwiązaniem posiadanym ani realizować funkcji w ten sam sposób. Za równoważne uznaje się rozwiązanie, które spełnia każde z wymagań wymienionych w tabeli kryteriów równoważności dla danej części. Katalog kryteriów jest zamknięty – Zamawiający nie będzie oceniał równoważności na podstawie wymagań niewymienionych w tabeli.

Wykonawca oferujący rozwiązanie równoważne (Wariant B) składa wraz z ofertą przedmiotowe środki dowodowe):

1) wypełnioną tabelę zgodności z kryteriami równoważności (wzór w formularzu ofertowym – załącznik nr 1 do Rozdziału I SWZ), ze wskazaniem dla każdego kryterium dokumentu i strony/rozdziału dokumentacji producenta, która potwierdza spełnienie wymagania;
2) oświadczenie producenta lub autoryzowanego dystrybutora oferowanego oprogramowania potwierdzające zakres licencji, liczbę instancji/pojemność oraz poziom i okres wsparcia producenta;
3) wstępny harmonogram wdrożenia i migracji (rozdział II.5 / III.4 niniejszego opisu przedmiotu zamówienia).

Podkarpackie Centrum Innowacji Sp. z o.o. | ul. Teofila Lenartowicza 4 , 35-051 Rzeszów | www. pcinn.org | NIP: 8133765154 | REGON: 368953574 | KRS: 0000710883 |
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie | Kapitał Zakładowy: 502 000,00 zł

Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub będą one niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie. Wykonawca oferujący Wariant A składa wyłącznie oświadczenie producenta lub autoryzowanego dystrybutora, o którym mowa w pkt 2.

4. Wymagania

- Okres subskrypcji i wsparcia producenta: minimum 12 miesięcy, liczone od dnia następującego po dniu wygaśnięcia obecnej subskrypcji (Wariant A) albo od dnia podpisania protokołu odbioru wdrożenia (Wariant B).
- Licencje/subskrypcje mają być wystawione na Zamawiającego jako użytkownika końcowego i zarejestrowane na jego koncie w portalu producenta (jeśli producent prowadzi taki portal).
- Dostawa w formie elektronicznej (klucze, potwierdzenia rejestracji kontraktu) na adres e-mail wskazany w umowie, nie później niż 5 dni roboczych przed datą wygaśnięcia obecnej subskrypcji.
- Wsparcie producenta obejmuje prawo do aktualizacji oprogramowania (w tym nowych wersji) oraz zgłaszania incydentów przez cały okres subskrypcji.
- Wykonawca dostarczy oprogramowanie pochodzące z oficjalnego kanału dystrybucji producenta na terenie EOG.

5. Zasady horyzontalne i wytyczne DNSH

1) Przedmiotem zamówienia jest oprogramowanie służące do tworzenia kopii zapasowych lub centralnego logowania, raportowania i korelacji zdarzeń. Funkcje administracyjne oprogramowania są przeznaczone do użytku przez personel IT Zamawiającego. Zamawiający nie uznaje oprogramowania za produkt pozbawiony bezpośrednich użytkowników wyłącznie dlatego, że nie korzystają z niego odbiorcy usług Zamawiającego.
2) Klucze licencyjne, potwierdzenia odnowienia subskrypcji oraz dokumentacja przewidziana w OPZ są przekazywane elektronicznie. Zamówienie nie obejmuje dostawy fizycznych nośników oprogramowania ani dokumentacji drukowanej.
3) W przypadku zaoferowania rozwiązania równoważnego oprogramowanie musi umożliwiać realizację funkcji określonych w OPZ z wykorzystaniem infrastruktury Zamawiającego wskazanej dla danej części zamówienia, zgodnie z wymaganiami dotyczącymi wdrożenia i równoważności. Zamawiający nie wymaga dostawy nowego sprzętu w ramach tego zamówienia.

II. System centralnego logowania, raportowania i korelacji zdarzeń

1. Stan posiadany

Posiadane oprogramowanie	FortiAnalyzer-VM, licencja 5 GB/dzień, uruchomiony na posiadanym środowisku Hyper-V
Data wygaśnięcia obecnej subskrypcji	31.10.2026
Posiadane usługi towarzyszące	FortiCare 24×7; FortiGuard Indicators of Compromise; FortiGuard Outbreak Detection
Informacyjnie – numer katalogowy posiadanego produktu	FC1-10-AZVMS-465-01-12 (charakter informacyjny, zob. rozdz. I.2)
Źródło logów	1 × Fortinet FortiGate, FortiOS 7.2.x lub nowszy
Obecny wolumen logów	ok. 2 GB/dzień (średnio)

Podkarpackie Centrum Innowacji Sp. z o.o. | ul. Teofila Lenartowicza 4 , 35-051 Rzeszów | www. pcinn.org | NIP: 8133765154 | REGON: 368953574 | KRS: 0000710883 |
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie | Kapitał Zakładowy: 502 000,00 zł

2. Wariant A – odnowienie posiadanej subskrypcji

Przedłużenie na 12 miesięcy licencji FortiAnalyzer-VM na przyjmowanie 5 GB logów dziennie wraz z kontraktem wsparcia producenta FortiCare 24×7 oraz usługami towarzyszącymi wymienionymi w pkt 1, z zachowaniem ciągłości względem daty wygaśnięcia.

3. Wariant B – kryteria równoważności

Rozwiązanie równoważne musi spełniać łącznie wszystkie poniższe wymagania.

Lp.	Wymaganie (kryterium równoważności)	Sposób wykazania
B2.1	Dostarczone w postaci maszyny wirtualnej uruchamianej na posiadanym środowisku Microsoft Hyper-V (Windows Server 2019/2022) lub jako oprogramowanie na dostarczonej przez Wykonawcę VM z systemem Linux/Windows; wszystkie komponenty i licencje niezbędne do działania objęte ceną oferty.	Dokumentacja producenta
B2.2	Przyjmowanie i indeksowanie co najmniej 5 GB logów dziennie od co najmniej 4 źródeł, z możliwością rozbudowy licencji o kolejne źródła i wolumen.	Oświadczenie producenta/dystrybutora
B2.3	Odbiór logów z posiadanego urządzenia FortiGate (FortiOS 7.2.x i nowszy) przez syslog (UDP/514 i TCP/514, opcjonalnie TLS) lub protokół natywny producenta, z rozpoznawaniem (parsowaniem) pól logu FortiOS co najmniej: identyfikator i nazwa polityki, adresy i porty źródłowe/docelowe, użytkownik, aplikacja, kategoria URL, kraj docelowy, sygnatura IPS/AV, status tunelu IPsec/SSL-VPN.	Dokumentacja producenta (lista wspieranych źródeł / parserów)
B2.4	Retencja logów przeszukiwalnych online przez min. 90 dni oraz archiwum przez min. 180 dni, przy posiadanym wolumenie; obsługa dysku VM o pojemności min. 2 TB.	Dokumentacja producenta
B2.5	Podgląd zdarzeń w czasie rzeczywistym oraz przeszukiwanie logów historycznych z filtrowaniem po dowolnym sparsowanym polu i zakresie czasu.	Dokumentacja producenta
B2.6	Predefiniowane widoki/raporty obejmujące co najmniej: najczęściej wykrywane ataki (IPS/AV), najbardziej aktywnych użytkowników i hosty, najczęściej używane aplikacje, najczęściej odwiedzane strony WWW, kraje docelowe połączeń, najczęściej wykorzystywane polityki firewall, stan tuneli VPN.	Dokumentacja producenta
B2.7	Generowanie raportów w formatach PDF i CSV, cyklicznie (harmonogram) lub na żądanie, z automatyczną wysyłką e-mail; możliwość tworzenia własnych raportów i modyfikacji predefiniowanych; możliwość nadawania polskich nazw i opisów raportom.	Dokumentacja producenta
B2.8	Korelacja zdarzeń i alarmowanie e-mail oraz SNMP dla zdefiniowanych reguł, w tym co najmniej: wykrycie malware/IPS, utrata połączenia VPN, utrata łączności z monitorowanym urządzeniem, przekroczenie progu liczby zdarzeń danej kategorii w czasie.	Dokumentacja producenta
B2.9	Przekazywanie kopii logów (log forwarding) do zewnętrznego systemu przez syslog z możliwością filtrowania oraz cykliczny eksport/archiwizacja logów na zewnętrzny zasób (SFTP lub udział sieciowy SMB/NFS – np. na posiadany NAS Synology).	Dokumentacja producenta

Lp.	Wymaganie (kryterium równoważności)	Sposób wykazania
B2.10	Zarządzanie przez HTTPS oraz SSH (lub dedykowaną konsolę producenta komunikującą się szyfrowanym protokołem); uwierzytelnianie administratorów: lokalne oraz LDAP/Active Directory lub RADIUS; MFA dla kont administracyjnych.	Dokumentacja producenta
B2.11	Co najmniej 4 konta administracyjne z rozdziałem uprawnień (RBAC) w zakresie dostępu do logów, raportów i konfiguracji.	Dokumentacja producenta
B2.12	System zapewnia automatyczne dopasowywanie przychodzących logów do wskaźników kompromitacji (adresy IP, domeny, hashe) aktualizowanych nie rzadziej niż raz na dobę, retrospektywne przeszukanie logów historycznych po aktualizacji bazy wskaźników oraz alarmowanie e-mail przy dopasowaniu. Źródło wskaźników może pochodzić od producenta oprogramowania albo od dostawcy zewnętrznego. Wykonawca dostarcza, konfiguruje i opłaca działające źródło wskaźników na cały 12-miesięczny okres objęty zamówieniem, w cenie oferty. Sposób wykazania: oświadczenie producenta lub dostawcy wskaźników wraz ze wskazaniem nazwy źródła i częstotliwości aktualizacji.	Oświadczenie producenta/dystrybutora
B2.13	System jest wyposażony w reguły korelacji lub sygnatury wykrywające znane zagrożenia, aktualizowane przez producenta oprogramowania lub dostawcę nie rzadziej niż raz w miesiącu przez cały 12-miesięczny okres objęty zamówieniem, w cenie oferty. Aktualizacja reguł nie może wymagać ręcznego ich tworzenia przez Zamawiającego. Sposób wykazania: dokumentacja producenta lub oświadczenie producenta albo dostawcy określające częstotliwość aktualizacji.	Oświadczenie producenta/dystrybutora
B2.14	Wsparcie producenta przez 12 miesięcy w trybie 24×7, obejmujące aktualizacje oprogramowania i zgłaszanie incydentów.	Oświadczenie producenta/dystrybutora

4. Obowiązki Wykonawcy przy Wariancie B (wdrożenie i migracja)

1) Instalacja i konfiguracja systemu, podłączenie posiadanego FortiGate jako źródła logów, konfiguracja raportów cyklicznych, reguł korelacji i powiadomień odpowiadających obecnie używanym.
2) Zapewnienie dostępu do dotychczasowych logów przez okres 12 miesięcy od odbioru – przez import archiwum do nowego systemu albo przez utrzymanie dotychczasowego systemu w trybie tylko-odczyt na koszt Wykonawcy.
3) Szkolenie do 2 osób wskazanych przez Zamawiającego w wymiarze min. 6 godzin; dokumentacja powykonawcza w języku polskim.
4) Termin zakończenia wdrożenia i odbioru: nie później niż 30 dni od podpisania umowy. Do tego dnia wszystkie prace wdrożeniowe muszą być wykonane w sposób niezakłócający działania obecnego systemu logowania. Wykonawca zapewnia ciągłość działania obecnego systemu logowania (w tym ważność jego subskrypcji i wsparcia producenta) do dnia odbioru na własny koszt.

III. Odbiór

- Wariant A: odbiór następuje na podstawie potwierdzenia rejestracji odnowionej subskrypcji na koncie Zamawiającego w portalu producenta (lub równoważnego dokumentu producenta/dystrybutora) i widoczności nowej daty ważności w konsoli oprogramowania.
- Wariant B: odbiór następuje po pozytywnym wyniku testów opisanych w rozdz. II.4, przekazaniu dokumentacji i przeprowadzeniu szkolenia, protokołem odbioru podpisanym przez obie strony.

Podkarpackie Centrum Innowacji Sp. z o.o. | ul. Teofila Lenartowicza 4 , 35-051 Rzeszów | www. pcinn.org | NIP: 8133765154 | REGON: 368953574 | KRS: 0000710883 |
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie | Kapitał Zakładowy: 502 000,00 zł