ZMIANA TREŚCI SWZ nr 1

A. Postępowanie nr: RGK.271.1.2026

Nazwa postępowania: Dostawa sprzętu i oprogramowania teleinformatycznego w ramach projektu „Cyberbezpieczny Samorząd”

B. Działając na podstawie art. 286 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, Zamawiający dokonuje zmiany treści SWZ/OPZ w następującym zakresie:

Zmiana nr 1 - nazwy punktu

W Spisie treści oraz w treści OPZ:

- dotychczasowy pkt **7. „Rozwiązanie do zbierania i analizowania danych z urządzeń sieciowych – 1 szt.”**
  otrzymuje brzmienie:
  „7. System kontroli dostępu NAC – 1 szt.”

Zmiana nr 2 – zmiana treści punktu 9 oraz nazwy

- dotychczasowy pkt **9. „System kontroli dostępu NAC – 1 szt.”**
  otrzymuje nazwę:
  „9. Rozwiązanie do zbierania i analizowania danych z urządzeń sieciowych – 1 szt.”

- oraz otrzymuje następujące brzmienie:

9. Rozwiązanie do zbierania i analizowania danych z urządzeń sieciowych – 1 szt.

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Wymagania ogólne	• Centralny system logowania, raportowania i korelacji zdarzeń umożliwiający centralizację logów sieciowych, systemowych i bezpieczeństwa. • Rozwiązanie komercyjne działające jako maszyna wirtualna lub platforma bazująca na systemie Linux w środowisku wirtualnym. • Możliwość uruchomienia na hypervisorach: VMware ESX/ESXi 5.0–6.7, Microsoft Hyper-V 2008 R2–2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS, Microsoft Azure, Google Cloud (GCP).

Interfejsy i zasoby	• Obsługa minimum 4 interfejsów sieciowych. • Obsługa przestrzeni dyskowej o pojemności minimum 3 TB.
Parametry wydajnościowe	• Możliwość przyjmowania minimum 5 GB logów dziennie. • Możliwość kolekcjonowania logów z minimum 1000 systemów/urządzeń.
Logowanie	• Podgląd logów w czasie rzeczywistym. • Przeglądanie logów historycznych z funkcją filtrowania. • Predefiniowane lub konfigurowalne raporty obejmujące co najmniej: najczęściej wykrywane ataki, najbardziej aktywnych użytkowników, najczęściej wykorzystywane aplikacje, najczęściej odwiedzane strony WWW, kraje docelowe połączeń, najczęściej wykorzystywane polityki Firewall, informacje o połączeniach IPSec. • Możliwość przesyłania kopii logów do innych systemów (z mechanizmem filtrowania). • Obsługa przyjmowania logów przez UDP/514 oraz TCP/514. • Cykliczny eksport logów do systemów zewnętrznych (SFTP lub zasób sieciowy).
Raportowanie	• Generowanie raportów w formatach minimum PDF oraz CSV. • Predefiniowane raporty z możliwością modyfikacji parametrów. • Możliwość definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów cyklicznych lub na żądanie. • Automatyczne wysyłanie raportów na wskazane adresy e-mail.
Korelacja logów	• Korelacja zdarzeń z możliwością wyboru urządzeń objętych korelacją. • Powiadomienia o zdarzeniach przez e-mail oraz SNMP. • Tworzenie reguł korelacyjnych dla co najmniej kategorii: Malware, Aplikacje sieciowe, Email, IPS, Traffic, Zdarzenia systemowe (utrata VPN, utrata połączenia sieciowego).
Zarządzanie i administracja	• Zarządzanie lokalne przez HTTPS i SSH lub dedykowaną konsolę szyfrowaną. • Uwierzytelnianie administratorów: lokalna baza, RADIUS, LDAP, PKI.

	• Możliwość zdefiniowania minimum 4 administratorów z różnymi poziomami uprawnień.
Serwisy i licencje	• Licencja bezterminowa (brak blokady działania po wygaśnięciu wsparcia). • Minimum 12 miesięcy wsparcia producenta 24/7 obejmującego aktualizacje i pomoc techniczną.
Wymagania formalne	• W przypadku produktów podwójnego zastosowania – dokument importera potwierdzający zgodność z przepisami prawa. • Oświadczenie producenta lub autoryzowanego dystrybutora o autoryzacji oferenta do sprzedaży rozwiązania.

C. Zmiana terminu składania ofert

W związku z istotną zmianą opisu przedmiotu zamówienia, termin składania ofert ulega zmianie:

- z dnia **24.02.2026 r. godz.09;00**
- na dzień **03.03.2026 r. godz. 09;00**

D. Pozostałe zapisy SWZ pozostają bez zmian.