Załącznik nr 1 do specyfikacji

Rozbudowa posiadanego systemu SIEM Splunk Enterprise o dodatkowe licencje wraz z instalacją, wdrożeniem subskrypcją i wsparciem na okres co najmniej do 14.12.2023r

I Rozbudowa posiadanego systemu SIEM Splunk Enterprise Perpetual, 20GB/day o licencje:

1. SPLUNK ENTERPRISE - DODATKOWE 20 GB/DAY - SUBSKRYPCJA - Splunk Enterprise - Term License with Standard Success Plan - GB/day
2. SPLUNK ENTERPRISE SECURITY - DODATKOWE 40 GB/DAY - SUBSKRYPCJA - Splunk Enterprise Security- Term License with Standard Success Plan - GB/day

II Instalacja i wdrożenie:

1. Splunk Enterprise:
    a. Zainstalowanie dodatkowych licencji Splunk Enterprise 20GB/day
2. Splunk Enterprise Security:
    a. Wykonanie analizy wymagań i projektu technicznego obejmującego między innymi:
        i. Szczegółową architekturę systemu (m.in.: komponenty, adresacja, komunikacja i integracja z zewnętrznymi aplikacjami)
        ii. Listę reguł detekcyjnych w systemie SIEM (do 40 reguł)
        iii. Lista źródeł logów i innych danych które będą analizowane w systemie SIEM
        iv. Instrukcję konfiguracji poszczególnych systemów i aplikacji podłączanych do SIEM
        v. Ogólne zasady procesu zarządzania incydentami wykrytymi przez system SIEM
    b. Instalacja dostarczonego oprogramowania SIEM oraz podstawowa konfiguracja parametrów
        i. Konfiguracja ról poszczególnych serwerów
        ii. Konfiguracja uwierzytelniania i ustawień kryptografii
        iii. Konfiguracja systemu z uwzględnieniem rekomendacji producenta oraz uwag Zamawiającego (jeśli takie będą)
        iv. Konfiguracja kopii bezpieczeństwa
    c. Podłączenie źródeł logów i innych danych oraz ich konfiguracja zgodnie z projektem technicznym:
        i. Konfiguracja indeksów
        ii. Konfiguracja danych i weryfikacja ich poprawności
        iii. Rekonfiguracja forwarderów zainstalowanych na systemach zewnętrznych
        iv. Konfiguracja pozostałych parametrów zgodnie z projektem technicznym oraz uwagami Zamawiającego (jeśli takie będą)
    d. Uruchomienie procesu zarządzania incydentami
        i. Integracja z AD i systemem pocztowym Exchange
        ii. Konfiguracja scenariuszy bezpieczeństwa wybranych w trakcie analizy wdrożenia (jeśli takie będą)
    e. Opracowanie dokumentacji powykonawczej obejmującej między innymi:
        i. Architekturę wdrożenia
        ii. Procedurę instalacji i aktualizacji systemu
        iii. Mechanizmy integracji z zewnętrznymi systemami oraz listę tych systemów
        iv. Konta i poświadczenia wykorzystywane do poprawnego działania systemu
        v. Procedury wykonywania kopii bezpieczeństwa/zapasowych oraz odtwarzania

vi. Procedury konfiguracji kont użytkowników

f. Na etapie całego etapu wdrożenia przekazywanie wiedzy administratorom Zamawiającego niezbędnej do późniejszego samodzielnego zarządzania systemem.

III Minimalne wymagania dotyczące wsparcia serwisowego:

1. możliwość zgłaszania awarii/usterki oprogramowania 24h 7 dni w tygodniu,
2. czas reakcji na zgłoszenie awarii/usterki oprogramowania – 4h od chwili zgłoszenia,
3. możliwość uaktualnienia oprogramowania do najnowszej zalecanej przez producenta wersji,
4. świadczenia asysty technicznej zapewniającej pomoc techniczną w przypadku niefunkcjonowania lub nieprawidłowego funkcjonowania oprogramowania,
5. pomoc przy rozwiązywaniu problemów z bieżącą eksploatacją oprogramowania.

IV Informacje dot. posiadanego systemu SIEM Splunk:

1. data zakończenia wsparcia serwisowego: w tracie przedłużania, przedłużenie do 14.12.2023

V Rozbudowa systemu SIEM Splunk Enterprise. Oferta równoważna

Użyte powyżej określenia wskazujące znaki towarowe, nazwy własne, lub pochodzenie przedmiotu zamówienia należy odczytywać wraz z wyrazami „lub równoważne”. Zamawiający dopuści możliwość instalacji systemu SIEM równoważnego w przypadku zachowania parametrów użytkowych, funkcjonalnych i jakościowych, które będą na poziomie nie niższym od parametrów wskazanych przez Zamawiającego w punkcie I i II oraz posiadanego przez Zmawiającego systemu SIEM Splunk Enterprise Perpetual 20GB/day (licencja wieczysta). .