Załącznik nr 6b

Opis Przedmiotu Zamówienia

Przedmiot zamówienia: Konfiguracja i wdrożenie systemu klasy SIEM

W ramach realizacji przedmiotu zamówienia, Wykonawca jest zobowiązany do kompleksowego wdrożenia systemu klasy SIEM Wazuh w środowisku Zamawiającego. Wdrożenie musi obejmować co najmniej następujące etapy i prace:

1. Analiza przedwdrożeniowa i projekt

- Przeprowadzenie inwentaryzacji infrastruktury Zamawiającego pod kątem dostępnych źródeł logów (dzienników zdarzeń).

- Opracowanie Projektu Technicznego Wdrożenia (PTW), uwzględniającego architekturę rozwiązania, polityki retencji (przechowywania) logów oraz wstępną listę scenariuszy użycia dopasowanych do środowiska Zamawiającego.

2. Instalacja i konfiguracja środowiska

- Instalacja niezbędnych komponentów systemu SIEM (węzły centralne, ewentualne kolektory logów, czujniki) na udostępnionej przez Zamawiającego infrastrukturze.

- Podstawowa konfiguracja parametrów systemowych, sieciowych oraz zabezpieczenie dostępu do samej platformy SIEM.

3. Integracja źródeł danych (Log collection) Podłączenie, weryfikacja odbioru i zapewnienie poprawnego parsowania (normalizacji) logów z infrastruktury Zamawiającego, obejmującej:

- Wszystkie urządzenia sieciowe i zabezpieczające dostarczane w ramach niniejszego postępowania (2 przełączniki rdzeniowe, 4 przełączniki dostępowe, 4 punkt dostępowy, 2 zapory sieciowe NGFW).

- Do 5 serwerów fizycznych.

- Do 10 maszyn wirtualnych (systemy operacyjne np. Windows Server, Linux).

- 1 macierz dyskową.

4. Konfiguracja logiki detekcji i korelacji zdarzeń

- Wdrożenie i uruchomienie co najmniej 20 predefiniowanych reguł korelacyjnych nakierowanych na wykrywanie incydentów (np. ataki brute-force, wielokrotne błędy logowania, skanowanie sieci, zmiany uprawnień administracyjnych, złośliwy ruch zablokowany przez NGFW).

- Opracowanie dedykowanych pulpitów menedżerskich i operacyjnych (Dashboardów) prezentujących bieżący stan bezpieczeństwa i kluczowe metryki.

- Skonfigurowanie mechanizmów automatycznego powiadamiania administratorów o wystąpieniu incydentów o wysokim priorytecie (np. poprzez wiadomości e-mail).

5. Testy, strojenie (Tuning) i optymalizacja

- Przeprowadzenie testów funkcjonalnych potwierdzających poprawność zbierania logów i wyzwalania alertów.

- Wykonanie tzw. strojenia (tuningu) wdrożonych reguł korelacyjnych przez okres minimum 14 dni od uruchomienia, w celu wyeliminowania zjawiska fałszywych alarmów (False Positives) i dostosowania alertów do specyfiki ruchu w sieci Zamawiającego.