

Część 7 – Wdrożenie oprogramowania SIEM

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Dostawa i wdrożenie Systemu klasy SIEM w architekturze Open Source

Rozdział 1: Cel i zakres zamówienia

1. Celem zamówienia jest dostawa, instalacja, konfiguracja i strojenie (tuning) Systemu klasy SIEM.
2. Oprogramowanie musi być udostępniane na licencji typu open source lub licencji komercyjnej gwarantującej wieczysty, bezpłatny dostęp do aktualizacji kodu i reguł bezpieczeństwa.
3. Zamówienie obejmuje pełne wdrożenie w architekturze klastrowej (High Availability) na infrastrukturze wirtualnej Zamawiającego, zapewniające redundancję funkcjonalną oraz replikację danych.

Rozdział 2: Harmonogram i Etapy Wdrożenia

Wdrożenie musi zostać zrealizowane w następujących etapach:

1. **Etap 1: Analiza przedwdrożeniowa i Projekt Techniczny.** Wykonawca przeprowadzi inwentaryzację środowiska IT Zamawiającego i opracuje Projekt Techniczny wdrożenia. Projekt musi zawierać obliczenie wymaganej mocy obliczeniowej CPU/RAM oraz przestrzeni dyskowej, gwarantujący płynne działanie systemu przy założeniu **24-miesięcznej retencji logów online/offline**.
2. **Etap 2: Instalacja i podstawowa konfiguracja.** Instalacja środowiska klastrowego, w tym węzłów przetwarzających (Manager/Worker) oraz klastra bazy danych/indeksowania na wskazanych przez Zamawiającego zasobach.
3. **Etap 3: Wdrażanie agentów i integracja źródeł logów.** Instalacja agentów na stacjach roboczych i serwerach (dopuszczalna dystrybucja masowa, np. via GPO lub SCCM). Integracja ze źródłami bezagentowymi (np. zapory sieciowe, systemy antywirusowe, IDS/IPS, usługi katalogowe).
4. **Etap 4: Strojenie (Tuning) i automatyzacja.** Konfiguracja reguł korelacyjnych opartych na frameworku MITRE ATT&CK, eliminacja tzw. *false-positives* (fałszywych alarmów) oraz wdrożenie zautomatyzowanych reakcji na incydenty bezpieczeństwa.
5. **Etap 5: Szkolenia, testy akceptacyjne (UAT) i Odbiór.** Przekazanie wiedzy oraz podpisanie bezusterkowego protokołu odbioru, co uruchamia okres wsparcia technicznego. Po wdrożeniu Wykonawca złoży oświadczenie, że system wspiera polityki zgodne z dyrektywą NIS2.

Rozdział 3: Szczegółowe parametry techniczne i funkcjonalne (Tabela Wymagań)

Poniższa tabela stanowi załącznik do weryfikacji ofert. Wykonawca musi potwierdzić spełnienie każdego z punktów.



Załącznik nr 1.7

Lp.	Grupa	Szczegółowe Wymaganie Funkcjonalne / Techniczne
1	Gromadzenie i Parsowanie Danych	Agregacja logów w czasie rzeczywistym ze stacji końcowych, urządzeń sieciowych, serwerów i środowisk chmurowych. Obsługa natywnych logów systemów Windows/Linux/macOS oraz protokołów Syslog, SNMP, JSON. System musi potrafić normalizować zdarzenia z różnych źródeł do ujednoliconego formatu.
2	Retencja i Integralność	Architektura systemu musi pozwalać na bezpieczne przechowywanie danych przez 2 lata (24 miesiące) w sposób zabezpieczający je przed nieautoryzowaną modyfikacją. Szyfrowanie komunikacji pomiędzy agentami a serwerem centralnym (TLS).
3	Silnik Korelacyjny i Detekcja	Analiza logów, detekcja anomalii i zagrożeń oparta na regułach zmapowanych do taktyk i technik MITRE ATT&CK . Wykrywanie ataków typu brute-force, zmian w plikach (FIM - File Integrity Monitoring) oraz korelacja ze skanerami podatności (CVE).
4	Reagowanie na Incydenty (SOAR/Active Response)	System musi posiadać natywne mechanizmy pozwalające na wykonanie zautomatyzowanej akcji zaradczej (np. zablokowanie IP na firewallu, wyłączenie konta w usługach katalogowych) lub posiadać udokumentowane API/Webhooks do integracji z zewnętrznymi platformami klasy SOAR.
5	Wizualizacja, Dashboardy i Raportowanie	Zintegrowany interfejs webowy oferujący spersonalizowane pulpity nawigacyjne z widżetami. Generowanie raportów na żądanie i okresowych (eksport do PDF/CSV), dostosowanych pod kątem zgodności z regulacjami takimi jak RODO, PCI-DSS czy NIS2. Obsługa ról użytkowników (RBAC: administrator, analityk, audytor).

Załącznik nr 1.7

6	Wydajność Architektura HA i	System musi działać w trybie klastrowym (multi-node) gwarantującym wysoką dostępność i load-balancing. Awaria pojedynczego węzła nie może powodować utraty logów ani przerw w monitorowaniu. Interfejs zarządzający nie może wymagać zakupu dodatkowych licencji komercyjnych.
7	Integracja ze Środowiskiem	Integracja z Active Directory w celu zarządzania uprawnieniami do samego systemu SIEM oraz monitorowania zdarzeń z kontrolerów domeny. Łatwa aktualizacja i rozbudowa infrastruktury monitorującej.

Rozdział 4: Warunki Szkoleń (Transfer Wiedzy)

Wykonawca zrealizuje zaawansowane warsztaty autoryzowane lub autorskie dla wyznaczonych administratorów i analityków (min. 2 osoby). Szkolenie (min. 16 godzin zegarowych) musi obejmować:

1. Zarządzanie architekturą klastra (w tym procedury backupu bazy danych i odtwarzania po awarii Disaster Recovery).
2. **Samodzielne wdrażanie nowych agentów i integrację nowych źródeł logów bezagentowych.**
3. Zarządzanie cyklem życia logów (konfiguracja polityk retencji danych i archiwizacji).
4. Tworzenie własnych parserów, dekodery i reguł korelacyjnych.
5. Tworzenie niestandardowych wizualizacji i dashboardów.
6. Obsługę alertów bezpieczeństwa, interpretację zdarzeń oraz konfigurację Active Response.

Rozdział 5: Gwarancja, SLA i Wsparcie Techniczne

1. **Podstawowy Okres Wsparcia:** Świadczony przez 12 miesięcy od dnia podpisania bezusterkowego protokołu odbioru.
2. **Warunki brzegowe wsparcia (SLA):**
 - o Wsparcie realizowane w dni robocze (pon.-pt.) w godz. 7:30-15:30.
 - o Brak limitu liczby zgłoszeń (incydentów, problemów, zapytań).
 - o Zakres wsparcia obejmuje m.in.: analizę błędów działania systemu, pomoc przy błędach konfiguracji, **asystę przy aktualizacji wersji oprogramowania SIEM** oraz aktualizację wbudowanych baz wiedzy (np. bazy podatności, reguły detekcji).
3. **Czasy reakcji i naprawy:**
 - o **Błąd Krytyczny (Niedostępność systemu lub utrata logów):** Czas reakcji max. 8 godziny robocze, czas przywrócenia funkcjonalności (obejście) max. 24 godzin roboczych.
 - o **Błąd Standardowy (Błąd funkcji niepowodujący zatrzymania monitorowania):** Czas reakcji max. 24 godzin roboczych.
 - o **Zapytanie techniczne/pomoc:** Czas reakcji max. 4 dni robocze.

Rozdział 6: Dokumentacja Powdrożeniowa

W terminie do 14 dni przed planowanym zgłoszeniem gotowości do odbioru końcowego, Wykonawca przedłoży w języku polskim kompletną Dokumentację Powdrożeniową. Dokumentacja musi składać się z dwóch głównych części: Dokumentacji Architektury oraz Katalogu Procedur Eksploatacyjnych.

6.1. Dokumentacja Architektury

Dokument musi w sposób wyczerpujący opisywać wdrożone środowisko, w tym:

1. Logiczny i fizyczny schemat architektury klastra SIEM (węzły centralne, indeksujące, agenty).
2. Konfigurację sieciową, wykaz wykorzystywanych portów, protokołów oraz reguł na zaporach sieciowych (Firewall).
3. Wykaz zintegrowanych systemów i źródeł logów (np. Active Directory, systemy antywirusowe, zapory sieciowe, IDS/IPS).
4. Zestawienie skonfigurowanych ról użytkowników (RBAC) i matrycę uprawnień.
5. Sposób realizacji wymogu 24-miesięcznej retencji danych (podział na warstwy danych np. Hot/Warm/Cold, lokalizacje zasobów dyskowych).

6.2. Katalog Procedur Eksploatacyjnych

Wykonawca opracuje i dostarczy szczegółowe instrukcje krok po kroku (wraz ze zrzutami ekranu lub fragmentami poleceń CLI), umożliwiające administratorom Zamawiającego samodzielne wykonywanie kluczowych zadań administracyjnych. Katalog musi zawierać minimum następujące procedury:

1. **Procedura aktualizacji systemu i komponentów (Patch Management):**
 - o Instrukcja bezpiecznego wdrażania aktualizacji (minor i major) dla głównego oprogramowania SIEM (Manager/Worker).
 - o Instrukcja masowej i jednostkowej aktualizacji agentów na stacjach końcowych i serwerach Zamawiającego.
 - o Instrukcja aktualizacji systemu operacyjnego (OS), na którym posadowione są komponenty SIEM.
 - o Procedura awaryjna (Rollback/Disaster Recovery) – instrukcja przywracania systemu do stanu sprzed aktualizacji w przypadku awarii (np. z wykorzystaniem snapshotów maszyn wirtualnych).
2. **Procedura zarządzania i aktualizacji bazy danych / silnika indeksującego:**
 - o Instrukcja utrzymania bazy danych (optymalizacja, przebudowa indeksów).
 - o Procedura zarządzania cyklem życia logów (Data Lifecycle Management) gwarantująca nieprzerwane zachowanie 24-miesięcznej retencji.
 - o Instrukcja wykonywania i weryfikacji kopii zapasowych (Backup & Restore) bazy danych i konfiguracji systemu.
3. **Procedura dodawania nowych źródeł danych (Data Onboarding):**
 - o Instrukcja instalacji i konfiguracji agentów na nowych systemach (Windows, Linux, macOS) krok po kroku.
 - o Instrukcja podłączania źródeł bezagentowych (np. urządzeń sieciowych, nowych firewalli) wykorzystujących protokoły Syslog, SNMP, JSON oraz API.
 - o Instrukcja tworzenia i modyfikacji reguł parsowania (dekoderów) w przypadku pojawienia się w sieci Zamawiającego nietypowych, nowych logów aplikacyjnych.

Załącznik nr 1.7

4. Procedura reagowania na incydenty i zarządzania alertami:

- Tworzenie własnych reguł korelacyjnych zgodnych z modelem MITRE ATT&CK.
- Instrukcja modyfikacji i tworzenia nowych pulpitów nawigacyjnych (Dashboardów).
- Konfiguracja zautomatyzowanych reakcji na zdarzenia (Active Response).