

Opis Przedmiotu Zamówienia / Specyfikacja techniczna

(Cz. I zamówienia)

Dostawa i wdrożenie Systemu typu Open Source służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management), zwanego dalej Systemem SIEM np. rozwiązanie klasy Wazuh lub równoważne spełniające wymagania minimalne w tabeli poniżej. Rozwiązanie na licencji open-source, umożliwiające agregację i analizę logów w czasie rzeczywistym z urządzeń końcowych, sieciowych oraz chmurowych, detekcję zagrożeń poprzez reguły oparte na frameworku MITRE ATT&CK, automatyzację reakcji na incydenty (integracja z SOAR, np. Shuffle), monitorowanie zgodności z regulacjami (RODO, PCI-DSS).

Przedmiotem zamówienia jest:

1. Wykonanie przez Wykonawcę projektu technicznego wdrożenia Systemu SIEM. "Dostarczenie do lokalizacji Zamawiającego Systemu SIEM (rozwiązanie klasy Wazuh lub równoważne), spełniającego minimalne wymagania techniczne określone w tabeli poniżej. Zapewnienie aktywacji subskrypcji Systemu SIEM w systemach serwisowych producenta. Wykonawca otrzyma dostęp administracyjny do wirtualizatora w celu instalacji systemu. System musi być wdrożony w architekturze rozproszonej, z zapewnieniem wysokiej dostępności (HA) oraz integracją z infrastrukturą Zamawiającego. Wymaga się, aby architektura systemu umożliwiała działanie w trybie klastrowym (multi-node) z redundancją funkcjonalną oraz replikacją danych dla wszystkich kluczowych komponentów. Przeprowadzenie warsztatów i dokumentacji powdrożeniowej. Dokumentacja powdrożeniowa powinna zawierać opis architektury, konfiguracji komponentów, listę integracji, zastosowane reguły bezpieczeństwa oraz zalecenia eksploatacyjne.
2. Instalacja i konfiguracja komponentów Systemu SIEM, w tym Dashboardu oraz Agentów na wskazanych hostach. Konfiguracja agentów może być przeprowadzona ręcznie lub w sposób zautomatyzowany, np. z wykorzystaniem GPO (Group Policy Objects) co obejmuje analizę logów, wykrywanie włamań, monitorowanie integralności plików, detekcję anomalii i reakcje na incydenty. System powinien integrować się z usługami katalogowymi w celu monitorowania zdarzeń i zarządzania uprawnieniami. Wymagana jest także integracja z systemami bezpieczeństwa (np. zapory sieciowe, systemy antywirusowe, IDS/IPS) w celu poszerzenia źródeł danych i automatyzacji reakcji. Wykonawca skonfiguruje automatyczne reakcje na zdarzenia oraz przygotowuje dashboardy i raporty dla różnych grup użytkowników. System musi być odpowiednio zabezpieczony: dostęp oparty o role, szyfrowanie komunikacji oraz audyt dostępu.
3. Wykonawca oświadczy po wdrożeniu, że wdrożony system umożliwia realizację polityk bezpieczeństwa zgodnych z NIS2, w tym przez dostarczenie odpowiednich konfiguracji oraz dokumentacji wspierającej ocenę zgodności, gwarantujące możliwie najwyższy poziom bezpieczeństwa.

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Wykonawca zapewni podstawowy okres wsparcia technicznego od dnia podpisania bezusterkowego, protokołarnego odbioru przedmiotu zamówienia do dnia 30 czerwca 2026 r. oraz w okresie 12 miesięcy od zakończenia podstawowego okresu, tj. od dnia 01 lipca 2026 r. Wsparcie techniczne w dni robocze (poniedziałek–piątek) w godzinach 7:30–15:30. Wsparcie nie może być limitowane liczbą zgłoszeń. Wsparcie techniczne obejmuje również aktualizacje i pomoc przy błędach konfiguracji.

Lp.	Minimalne wymaganie funkcjonalne	Nie potrzebne skreślić*
1	Agregacja i analiza logów w czasie rzeczywistym z urządzeń końcowych, sieciowych oraz chmurowych	Spełnia / Nie spełnia*
2	Detekcja zagrożeń poprzez reguły oparte na frameworku MITRE ATT&CK	

3	Automatyzacja reakcji na incydenty (integracja z SOAR, np. Shuffle)	Spełnia / Nie spełnia*
4	Monitorowanie zgodności z regulacjami (RODO, PCI-DSS)	
5	Oprogramowanie typu open source lub licencja komercyjna z wieczystym bezpłatnym dostępem do aktualizacji	
6	Gromadzenie, korelacja zdarzeń z innych systemów	
7	Monitorowanie zdarzeń bezpieczeństwa	
8	Analiza logów i detekcja anomalii	
9	Reakcja na zagrożenia i alertowanie personelu	
10	Kompatybilność z istniejącą infrastrukturą IT	
11	Możliwość rozszerzenia funkcjonalności	
12	Zgodność z regulacjami: PCI DSS, HIPAA, NIST 800-53, TSC GDPR	
13	Zbieranie logów z różnych źródeł	
14	Zestaw reguł detekcji zgodnych z branżowymi standardami	
15	Generowanie alertów na podstawie zagrożeń	
16	Reakcje automatyczne na zdarzenia	
17	Integracja z systemami ticketingowymi	
18	Analiza trendów i podejrzanych wzorców	
19	Szyfrowanie komunikacji między komponentami	
20	Zabezpieczenia dostępu do systemu	
21	Intuicyjny interfejs zarządzania	

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

22	Łatwa aktualizacja i rozbudowa	Spełnia / Nie spełnia*
23	Integracja z różnymi systemami (serwery, firewalle, IDS, NAC, AD)	
24	Obsługa protokołów: Syslog, SNMP, WMI	
25	Normalizacja i korelacja logów z różnych źródeł	
26	Przypisanie poziomów krytyczności zasobom	
27	Mapowanie zdarzeń do framework MITRE ATT&CK	
28	Automatyczne powiadamianie o incydentach	
29	Korelacja z anomaliami w przepływach sieciowych i skanerami CVE	
30	Detekcja zagrożeń na poziomie hosta (HIDS)	
31	Wykrywanie ataków brute-force i zmian w plikach	
32	Detekcja zagrożeń na poziomie sieci (NIDS)	
33	Analiza ruchu w czasie rzeczywistym i danych archiwalnych	
34	Centralne zarządzanie politykami bezpieczeństwa	
35	Konfiguracja wielu agentów	
36	Integracja z Elastic Stack (Elasticsearch, Logstash, Kibana)	
37	Raportowanie i wizualizacja danych bezpieczeństwa	
38	Tworzenie niestandardowych raportów	
39	Monitorowanie integralności plików (FIM)	
40	Konfiguracja zautomatyzowanych reakcji	
41	Obsługa protokołów: Syslog, SNMP, JSON	
42	Moduły i rozszerzenia systemu	
43	Generowanie raportów na żądanie i okresowych	
44	Raporty dostosowane do różnych odbiorców	
45	Bezpieczne przechowywanie logów przez min. 1 rok	
46	Ochrona danych przed nieautoryzowanym dostępem	
47	Spersonalizowane pulpity nawigacyjne z widżetami	
48	Eksport raportów do PDF/CSV	
49	Obsługa ról użytkowników (administrator, analityk, auditor)	

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.