OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) wraz ze wsparciem producenta, szkoleniem oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji wieczystych na system klasy SIEM (Security Information and Event Management), służący do centralnego gromadzenia, analizy i korelacji logów oraz zdarzeń bezpieczeństwa, dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wraz ze wsparciem producenta, szkoleniem oraz usługą wdrożenia i dodatkowym wsparciem powdrożeniowym.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencja wieczysta na system SIEM – zgodnie z rozdz. 2 i 3	2 kpl. (1 – sieć IT, 1 – sieć OT)
2.	Wsparcie producenta systemu SIEM dla obu instancji (IT i OT) – zgodnie z rozdz. 4	24 miesiące
3.	Szkolenie z użytkowania i administrowania systemem – zgodnie z rozdz. 5	2 pracowników, min. 8 godzin
4.	Usługa wdrożenia systemu SIEM w dwóch niezależnych sieciach IT i OT	1 usługa
5.	Dodatkowe wsparcie powdrożeniowe na prace rozwojowe i szkoleniowe	32 godziny robocze

1.4. Zamówienie obejmuje dostawę licencji dla dwóch instancji systemu SIEM: jednej przeznaczonej dla sieci IT i jednej dla sieci OT Zamawiającego. Instancje muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.5 i rozdz. 6. Wymagania z rozdz. 3 dotyczą każdej z instancji.

1.5. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 72268000-1 Usługi dostawy oprogramowania; 80533100-0 Usługi szkolenia w zakresie komputerów; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być licencjami wieczystymi (udzielonymi na czas nieoznaczony), wystawionymi na Zamawiającego. Licencja dla każdej z instancji musi obejmować co najmniej wydajność określoną w pkt 1 tabeli w rozdz. 3 i nie może ograniczać liczby użytkowników ani źródeł danych.

2.2. Po zakończeniu okresu wsparcia producenta każda z instancji musi nadal działać w pełnym zakresie funkcjonalnym, z wykorzystaniem ostatniej zainstalowanej wersji oprogramowania, bez konieczności ponoszenia dodatkowych opłat i bez ograniczenia wolumenu przyjmowanych danych.

2.3. System musi być instalowany w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Zamawiającego, odrębnym dla sieci IT i dla sieci OT. Działanie funkcji systemu, w tym licencjonowanie i aktywacja licencji, nie może wymagać stałego połączenia z chmurą producenta. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji oprogramowania i zawartości (parserów, reguł korelacyjnych, baz reputacyjnych IP, repozytorium IoC, baz podatności, modeli AI) w trybie offline.

2.4. Zamawiający zapewnia niezbędną infrastrukturę techniczną wymaganą do uruchomienia systemu. Strony określą wymagania dotyczące niezbędnego środowiska produkcyjnego na etapie tworzenia projektu technicznego.

2.5. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własną bazą danych, kontami użytkowników, konfiguracją i licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami.

Zamawiający nie dopuszcza realizacji separacji sieci IT i OT wyłącznie w trybie multi-tenant (pkt 106 tabeli) w ramach jednej instancji. Funkcja centralnego dostępu do instancji (pkt 116 tabeli) nie będzie wykorzystywana do łączenia instancji IT i OT.

2.6. Funkcje wykorzystujące model językowy (pkt 33–41 oraz 125 tabeli) muszą być możliwe do uruchomienia z modelem działającym lokalnie w infrastrukturze Zamawiającego. Korzystanie z modelu w chmurze producenta lub z zewnętrznych modeli językowych (pkt 34 tabeli) wymaga uprzedniej pisemnej zgody Zamawiającego i musi być możliwe do całkowitego wyłączenia. W instancji OT dopuszcza się wyłącznie model lokalny albo wyłączenie tych funkcji.

2.7. System musi być dostarczony w najnowszej wersji dostępnej na dzień dostawy. Dokumentacja musi być dostępna w języku polskim lub angielskim (dopuszcza się wersję elektroniczną).

2.8. Licencje i wsparcie muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej. Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację wsparcia u producenta na rzecz Zamawiającego.

3. Wymagania funkcjonalne systemu SIEM

Oferowany system musi spełniać co najmniej poniższe wymagania minimalne, odrębnie w każdej z instancji (IT i OT).

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
A. Licencja i wydajność		
1.	System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie – w każdej z instancji (IT i OT).	
2.	Oferowana licencja nie może ograniczać liczby zarejestrowanych lub jednocześnie pracujących użytkowników systemu.	
3.	Licencja na oferowany system nie może ograniczać liczby źródeł danych, z których pobierane są dane i zdarzenia.	
4.	System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 24 miesięcy.	
5.	System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o co najmniej 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.	
B. Wymagania ogólne		
6.	System musi być oparty o nowoczesną nierelacyjną bazę danych typu NoSQL.	
7.	System musi pracować w oparciu o system operacyjny z rodziny Linux.	
8.	System musi mieć możliwość centralnego zbierania i zarządzania logami.	
9.	System musi działać w trybie zbliżonym do czasu rzeczywistego.	
10.	System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych i nieudanych logowań, pełnej historii operacji, realizowanych zapytań oraz zmian uprawnień.	
11.	System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.	
12.	System musi posiadać autoryzowane przez producenta narzędzie (moduł) do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować swoim zakresem również to narzędzie.	
13.	System musi posiadać wbudowaną funkcjonalność analizy zachowania użytkowników oraz urządzeń (UEBA), opartą na danych pochodzących ze zgromadzonych logów, analizowanych za pomocą algorytmów sztucznej inteligencji.	
14.	Oferowana funkcjonalność UEBA musi zawierać wbudowane wizualizacje, kokpity oraz zestawy predefiniowanych modeli analizy opartych na algorytmach sztucznej inteligencji.	
15.	System musi zapewniać wizualizację danych w postaci oryginalnych logów, list, wykresów i diagramów.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
16.	System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w systemie danych.	
17.	Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.	
18.	System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.	
19.	System musi zapewniać funkcjonalność badania integralności plików i rejestrów na monitorowanych hostach, w tym: monitorowanie zmian zawartości plików i katalogów, zmian uprawnień dostępu do plików, zmian atrybutów plików oraz zmian sum kontrolnych MD5 i SHA1.	
20.	System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi utwardzania systemów (hardeningu), takimi jak CIS Benchmark.	
21.	System musi posiadać możliwość skanowania środowiska pod kątem wykrywania rootkitów oraz ukrytych procesów, plików i portów.	
22.	System musi posiadać funkcjonalność skanowania podatności aplikacji oraz systemów operacyjnych Linux i Windows.	
23.	System musi posiadać funkcjonalność ciągłego śledzenia zgodności z politykami OpenSCAP.	
24.	System musi umożliwiać integrację z MITRE ATT&CK.	
25.	System musi posiadać natywną integrację z bazą MISP w zakresie co najmniej: adresów IP, skrótów (hash) zainfekowanych plików, domen oraz adresów URL.	
C. Sztuczna inteligencja i uczenie maszynowe		
26.	System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.	
27.	System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne (tzw. Machine Learning).	
28.	System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.	
29.	Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez analizę liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).	
30.	Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Wykrywanie anomalii musi być połączone z obliczaniem punktacji, co umożliwi operatorowi skoncentrowanie pracy na zdarzeniach o najwyższych wynikach.	
31.	Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, tak aby można było łatwo zidentyfikować zdarzenia odosobnione.	
32.	Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, tak aby możliwa była szybka reakcja na pojawiające się sytuacje.	
33.	Oferowany system musi być wyposażony we wbudowany model językowy (LLM/GPT), dostarczony przez producenta i stanowiący integralną część oferowanej platformy. Model językowy musi działać lokalnie w infrastrukturze Zamawiającego lub w środowisku chmurowym należącym do producenta, z zapewnieniem zgodności z obowiązującymi u Zamawiającego wymaganiami w zakresie bezpieczeństwa i ochrony danych.	
34.	System musi umożliwiać integrację z zewnętrznymi modelami językowymi, takimi jak OpenAI, Fireworks, lub z modelem językowym (LLM) zgodnym ze standardem Ollama, z zachowaniem pełnej zgodności z obowiązującymi u Zamawiającego zasadami bezpieczeństwa i ochrony danych.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
35.	System musi umożliwiać zdefiniowanie kontekstu organizacyjnego Zamawiającego, w tym: wykorzystywanych technologii, struktury organizacyjnej oraz obowiązujących wymagań prawnych. Na podstawie wprowadzonych danych wbudowany model językowy (LLM) ma generować wyniki analizy dostosowane do specyfiki działalności Zamawiającego.	
36.	Wbudowany model językowy (LLM), stanowiący integralną część oferowanego systemu, musi umożliwiać dynamiczną analizę gromadzonych danych, w szczególności w zakresie: – automatycznego wyjaśnienia analizowanego zdarzenia, – weryfikacji potencjalnego naruszenia bezpieczeństwa wraz z rekomendacją działań naprawczych, – klasyfikacji wykrytego zagrożenia z wykorzystaniem matrycy MITRE ATT&CK, – opisu wektora ataku, – wykrycia naruszenia danych wrażliwych.	
37.	Oprogramowanie musi udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.	
38.	System musi umożliwiać rozbudowywanie funkcji Asystenta AI o nowe zapytania (prompty) w kontekście analizy logów. Utworzone zapytania muszą być dostępne dla wszystkich użytkowników systemu za pomocą nowych przycisków lub pozycji list rozwijanych.	
39.	Asystent AI musi umożliwiać budowanie odpowiedzi w dowolnym języku.	
40.	Asystent AI musi automatycznie dopasowywać zdarzenie do technik i taktyk matrycy MITRE ATT&CK.	
41.	Asystent AI musi automatycznie wyodrębniać obiekty IoC ze wskazanego rekordu logów.	
D. Parsowanie i analiza logów		
42.	System musi pozwalać na tworzenie parserów z poziomu interfejsu graficznego (GUI).	
43.	System musi posiadać predefiniowany zestaw parserów zdarzeń.	
44.	Wizualizacja danych powinna być możliwa zarówno dla wartości tekstowych, jak i liczbowych przekazywanych w logach.	
45.	System musi zapewniać parsowanie przesyłanych do niego wiadomości w formatach: – Syslog, – WEF, – Flat file, – Event log, – WMI, – SNMP trap, – XML, – JSON, – JDBC/ODBC, – CSV, – e-mail.	
46.	System musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby po stronie Zamawiającego.	
47.	System musi zbierać logi z rozwiązań chmurowych, co najmniej AWS oraz Microsoft Azure.	
48.	System musi umożliwiać gromadzenie danych z relacyjnych i nierelacyjnych (NoSQL) baz danych oraz systemów przetwarzania danych w czasie rzeczywistym, m.in. Microsoft SQL Server, Oracle, PostgreSQL, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka.	
49.	System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do systemu, tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
50.	System musi wykorzystywać do przyjmowania zdarzeń zarówno mechanizmy agentowe, jak i bezagentowe.	
51.	Operacje na rekordach bazy danych muszą być wykonywane wyłącznie za pomocą składni JSON z wykorzystaniem udokumentowanego API.	
52.	Dostęp do bazy danych musi odbywać się za pomocą REST API, bez wykorzystania klienta typu SQL client.	
53.	System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formaty wymiany danych, dla wszystkich obsługiwanych formatów.	
54.	System musi umożliwiać parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np. REGEX, JSON, XML, oraz umożliwiać zastosowanie innego parsera.	
55.	System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. poprzez zmianę wartości tych pól oraz wzbogacanie danych o dodatkowe pola na podstawie całych wartości lub wzorców wyszukiwania.	
56.	System musi umożliwiać przeszukiwanie danych wejściowych z uwzględnieniem filtrowania po sparsowanych polach.	
57.	Proces parsowania musi umożliwiać wzbogacanie treści odbieranych wiadomości poprzez operacje matematyczne wykonywane na innych polach.	
58.	Proces parsowania musi umożliwiać anonimizację danych wejściowych w celu ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzne procedury bezpieczeństwa.	
59.	System powinien pozwalać na pracę z logami zdarzeń jednowierszowych oraz wielowierszowych.	
60.	System powinien pozwalać na rozpoznawanie formatów daty i czasu oraz normalizowanie ich do jednego wspólnego formatu.	
61.	System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.	
E. Parsowanie i analiza ruchu sieciowego		
62.	System musi umożliwiać gromadzenie i analizowanie danych o przepływach sieciowych, w tym: NetFlow v9, IPFIX, sFlow, J-Flow.	
63.	System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.	
64.	System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, co najmniej dla protokołów HTTP, DNS, FTP oraz SSH.	
65.	System musi, na podstawie gromadzonej kopii ruchu sieciowego, identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników.	
66.	System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP.	
67.	System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, retransmisji, zmienności opóźnień (jitter), czasu odpowiedzi serwera (Server Response Time) oraz czasu podróży pakietu w obie strony (Round Trip Time).	
F. Korelacja danych i obsługa incydentów		
68.	System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.	
69.	System musi posiadać bazę co najmniej 700 predefiniowanych reguł korelacyjnych.	
70.	System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
71.	System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym: – wykrycia dowolnej treści w logach, – wykrycia wystąpienia wartości pola na wybranej liście, – wykrycia niewystępowania wartości pola na wybranej liście, – wykrycia zmiany jednego z kilku pól, – wykrycia zdarzeń występujących z zadaną częstotliwością, – wykrycia zdarzeń, których liczba zmienia się we wskazany sposób względem okresu poprzedniego, – wykrycia zaniku wiadomości, – wykrycia nowej wartości pola w zadanym okresie, – wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności.	
72.	System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej ani ewentualnego incydentu.	
73.	System musi posiadać funkcjonalność Bad IP Reputation, tj. porównywania adresów IP z bazami reputacyjnymi dostarczanymi przez producenta.	
74.	System musi wspierać geolokalizację zdarzeń na podstawie adresów IP.	
75.	System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.	
76.	System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL oraz Piped Processing Language (PPL).	
77.	Incydent, który powstał w wyniku korelacji, musi być możliwy do wyszukania za pomocą standardowego, dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowanie alarmów.	
78.	System musi pozwalać na tworzenie własnych algorytmów ewaluacji incydentów.	
79.	Reguły korelacyjne oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji zarówno z poziomu GUI, jak i API.	
80.	System musi pozwalać na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.	
81.	System musi umożliwiać korelację zdarzeń z różnych źródeł informacji z wykrytymi anomaliami, takimi jak dane NetFlow oraz podatności zidentyfikowane przez skaner podatności.	
82.	System musi zapewniać mechanizmy obsługi incydentów i wymiany informacji pomiędzy operatorami systemu, w tym przypisanie incydentu do operatora i zmianę jego statusu.	
83.	System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu (tzw. playbooków).	
84.	System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.	
85.	Scenariusze muszą mieć możliwość symulacji i weryfikacji, m.in. na przykładowym zasobie IT.	
86.	System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.	
87.	Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej powiadomienia e-mail, opcjonalnie SMS i komunikator).	
88.	System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. Rozwiązanie musi zapewniać kategoryzację obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni nadane wagi.	
89.	System musi umożliwiać konfigurację automatycznych akcji wykonywanych na monitorowanych systemach w przypadku wykrycia zagrożenia wskazanego w regule.	
90.	Incydenty tworzone w wyniku działania reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
91.	Musi istnieć możliwość automatycznego importu wskaźników kompromitacji (IoC, ang. Indicator of Compromise), a następnie automatycznego przeszukiwania zgromadzonych zdarzeń w wyznaczonym przedziale czasu.	
92.	System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.	
G. Retencja danych i archiwizacja		
93.	System musi zapewniać retencję danych online przez okres co najmniej 90 dni.	
94.	System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz zarządzanie archiwum z poziomu konsoli użytkownika.	
95.	Mechanizm archiwizacji musi umożliwiać przesyłanie danych online do archiwum według zadanych kryteriów, w sposób automatyczny lub ręczny.	
96.	Mechanizm archiwizacji musi umożliwiać przywracanie danych do systemu w celu analizy online.	
97.	Mechanizm archiwizacji musi zapewniać wyszukiwanie w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.	
H. Raportowanie		
98.	System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.	
99.	Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.	
100.	System musi generować raporty co najmniej w formatach PDF, DOCX oraz JPEG, z możliwością opatrzenia dokumentu logo Zamawiającego oraz komentarzami.	
101.	System musi umożliwiać eksport danych o zdarzeniach i incydentach do formatu CSV i HTML, m.in. w celu analizy wyników działania reguł korelacyjnych.	
102.	System musi posiadać gotowe wizualizacje i polityki zgodności z RODO (GDPR), PCI DSS oraz NIST.	
I. Dostęp do systemu		
103.	Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.	
104.	System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet.	
105.	Interfejs musi posiadać angielską lub polską wersję językową.	
106.	System musi zapewniać mechanizmy umożliwiające pracę w trybie multi-tenant.	
107.	System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej, co najmniej Firefox, Chrome, Microsoft Edge.	
108.	Dostęp do systemu musi być zabezpieczony hasłem lub certyfikatem.	
109.	Uwierzytelnianie w systemie musi być zintegrowane z: Microsoft Active Directory, LDAP, RADIUS.	
110.	Hasła konta używanego do powiązania z Active Directory (AD bind) muszą być przechowywane w postaci zaszyfrowanej.	
111.	System musi wspierać mechanizm logowania typu Single Sign-On.	
112.	System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.	
113.	System musi posiadać dedykowany widok zarządzania użytkownikami i rolami oparty o RBAC (Role-Based Access Control).	
114.	System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji obiektów wytworzonych w systemie, tj. wyszukiwań, wizualizacji, dashboardów. Dla utworzonych ról musi istnieć możliwość przypisania tych obiektów z dostępem typu „tylko odczyt” (read only) lub „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
J. Architektura		
115.	System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.	
116.	System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego, z możliwością centralnego dostępu.	
117.	Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery lub maszyny wirtualne). Należy przewidzieć rozdzielenie co najmniej 3 typów ról: agregacji, prezentacji i retencji.	
118.	System musi umożliwiać dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania danych, pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.	
119.	System powinien umożliwiać – jako funkcję opcjonalną – uruchomienie wysokiej dostępności (HA) dla warstw agregacji, retencji oraz prezentacji.	
120.	System musi zapewniać buforowanie agregowanych danych przez okres co najmniej 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie po przywróceniu pełnej sprawności systemu.	
121.	Komunikacja pomiędzy wszystkimi komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji co najmniej 1.3.	
122.	Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokół TLS w wersji co najmniej 1.3.	
K. Wymagania niefunkcjonalne i dokumentacja		
123.	System musi być tworzony zgodnie z zaleceniami OWASP Testing Guide, w szczególności OWASP Top 10 (Open Web Application Security Project). System powinien spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0, co najmniej na poziomie pierwszym (L1).	
124.	Producent systemu SIEM musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewniać gotową integrację z systemem SOAR tego samego producenta.	
125.	Oferowany system musi zapewniać dostęp do pełnej dokumentacji technicznej bezpośrednio z poziomu interfejsu użytkownika. Dokumentacja musi być możliwa do przeszukiwania z wykorzystaniem wbudowanego Asystenta AI (modelu językowego LLM), umożliwiającego formułowanie i wykonywanie zapytań w języku naturalnym.	

W celu potwierdzenia zgodności oferowanego rozwiązania z wymaganiami Zamawiający żąda złożenia wraz z ofertą:

- wypełnionej tabeli w załączniku nr 2.1 do formularza ofertowego, ze wskazaniem producenta, nazwy i wersji oferowanego systemu;
- dokumentacji producenta (np. karty produktu, dokumentacji technicznej, opisu licencjonowania) potwierdzającej spełnienie wymagań z rozdz. 3, w tym dostępność licencji wieczystej, model licencjonowania (EPS lub GB dziennie) oraz możliwość pracy i aktualizacji bez dostępu do Internetu (instancja OT);
- dokumentu potwierdzającego posiadanie przez producenta certyfikatu, o którym mowa w pkt 4.5.

Jeżeli z dokumentów producenta nie wynika jednoznacznie spełnienie danego wymagania, Wykonawca może złożyć oświadczenie producenta lub jego autoryzowanego przedstawiciela.

4. Wsparcie producenta

4.1. Wykonawca zapewni wsparcie producenta systemu SIEM dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji.

4.2. W ramach wsparcia producenta Zamawiający musi mieć zapewniony dostęp do nowych wersji oprogramowania, aktualizacji (poprawek) oraz repozytorium danych wskaźników kompromitacji (IoC).

Dla instancji OT producent musi udostępniać aktualizacje oprogramowania i zawartości w postaci pakietów do instalacji w trybie offline.

4.3. Wsparcie producenta musi być realizowane w języku polskim.

4.4. Wsparcie nie może być limitowane liczbą zgłoszeń.

4.5. Usługi utrzymania systemu świadczone przez producenta muszą być objęte certyfikowanym systemem zarządzania bezpieczeństwem informacji zgodnym z normą PN-EN ISO/IEC 27001:2017 lub ISO/IEC 27001:2022 albo równoważną.

4.6. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.

4.7. Producent oferowanego oprogramowania musi udostępniać otwarty portal dla społeczności użytkowników, z możliwością zadawania pytań wykraczających poza standardową usługę wsparcia.

4.8. Zgłoszenia przyjmowane są w dni robocze, przez portal producenta, e-mailem lub telefonicznie. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych.

5. Szkolenie

5.1. Wykonawca przeprowadzi szkolenie z zakresu użytkowania oraz administrowania systemem dla 2 pracowników Zamawiającego, w wymiarze co najmniej 8 godzin, obejmujące specyfikę obu instancji (IT i OT), w tym aktualizację instancji OT w trybie offline.

5.2. Grupa szkoleniowa będzie liczyła nie więcej niż 5 słuchaczy.

5.3. Szkolenie odbędzie się w siedzibie Zamawiającego, w terminie uzgodnionym z Zamawiającym.

5.4. Szkolenie musi być prowadzone w języku polskim.

5.5. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.

5.6. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania, potwierdzający ich kompetencje w zakresie użytkowania i administrowania systemem. Wykonawca przekaże kopie certyfikatów przed rozpoczęciem szkolenia.

6. Wdrożenie w sieciach IT i OT

6.2. Zasady wdrożenia w sieciach IT i OT

6.2.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję systemu SIEM, zgodnie z pkt 2.5.

6.2.2. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

6.2.3. Instancja IT będzie gromadzić dane wyłącznie ze źródeł działających w sieci IT, a instancja OT – wyłącznie ze źródeł działających w sieci OT. Źródła danych instancji OT wymagające dostępu do Internetu lub usług chmurowych (np. logi z AWS i Microsoft Azure – pkt 47 tabeli, zewnętrzne bazy reputacyjne i źródła IoC) zostaną wyłączone albo zastąpione źródłami lokalnymi, aktualizowanymi w trybie offline.

6.2.4. W sieci OT Wykonawca zastosuje bezpieczną konfigurację, w szczególności:

- dane z urządzeń sterowania procesem (m.in. sterowników PLC, RTU, serwerów SCADA, stacji HMI) będą pozyskiwane wyłącznie bezagentowo i pasywnie (np. syslog, SNMP trap, eksport z systemów nadrzędnych), bez instalowania oprogramowania na sterownikach PLC i RTU;
- agenty systemu (pkt 50 tabeli) zostaną zainstalowane wyłącznie na stacjach i serwerach wskazanych przez Zamawiającego, po potwierdzeniu zgodności z zaleceniami dostawców systemów sterowania;
- przechwytywanie i analiza pakietów (pkt 64 tabeli) będzie realizowana wyłącznie pasywnie, z portów SPAN lub urządzeń TAP wskazanych przez Zamawiającego;

- skanowanie podatności, wykrywanie rootkitów i monitorowanie konfiguracji (pkt 20–22 tabeli) będą uruchamiane wyłącznie na hostach wskazanych przez Zamawiającego i w uzgodnionych oknach serwisowych; aktywne skanowanie urządzeń sterowania procesem jest niedopuszczalne;
- automatyczne akcje na monitorowanych systemach (pkt 89 tabeli) zostaną wyłączone; w instancji OT system może jedynie generować alarmy i powiadomienia, a działania naprawcze wymagają decyzji upoważnionego operatora;
- funkcje AI korzystające z modelu w chmurze oraz zewnętrzne modele językowe zostaną wyłączone, zgodnie z pkt 2.6.

6.2.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym. Podłączanie źródeł danych w sieci OT poprzedzi instalacja pilotażowa na wskazanym przez Zamawiającego, ograniczonym zakresie źródeł.

6.3. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

6.3.1. Opracowanie harmonogramu wdrożenia systemu w obu sieciach.

6.3.2. Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

6.3.3. Przeprowadzenie instalacji i konfiguracji każdej z instancji, w tym konfiguracja ról i kont użytkowników (RBAC), integracji uwierzytelniania, szyfrowania TLS oraz utwardzenie konfiguracji (zmiana domyślnych haseł, wyłączenie zbędnych usług). Dla instancji OT – konfiguracja pracy bez dostępu do Internetu.

6.3.4. Podłączenie do każdej z instancji źródeł danych wskazanych przez Zamawiającego, działających w danej sieci.

6.3.5. Skonfigurowanie dla podłączonych źródeł reguł korelacyjnych, raportów oraz dashboardów z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.

6.3.6. Jeżeli oferowany system nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych dla wskazanych źródeł, Wykonawca jest zobowiązany do ich implementacji na etapie wdrożenia.

6.3.7. Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych, odrębnie dla sieci IT i dla sieci OT (dla sieci OT – z uwzględnieniem zdarzeń charakterystycznych dla sieci przemysłowych, np. nieautoryzowanych połączeń do segmentu sterowania, logowań do stacji inżynierskich i HMI, zmian konfiguracji).

6.3.8. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego, w każdej z sieci. Proponowane scenariusze zostaną przedłożone Zamawiającemu do akceptacji i muszą obejmować co najmniej:

- przyjęcie i sparsowanie zdarzeń z każdego typu podłączonego źródła oraz wygenerowanie incydentu przez skonfigurowaną regułę korelacyjną i wysłanie powiadomienia;
- przyjęcie danych z wydajnością określoną w pkt 2.1;
- buforowanie danych przy awarii komponentu i ich uzupełnienie po przywróceniu sprawności (pkt 120 tabeli);
- archiwizację i przywrócenie danych z archiwum;
- aktualizację instancji OT i jej zawartości w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu zarządzania, brak połączeń między instancjami IT i OT oraz – w sieci OT – brak aktywnych akcji na monitorowanych systemach.

6.3.9. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej opis architektury i konfiguracji, wykaz podłączonych źródeł danych i parserów, wykaz kont technicznych i ról, opis wdrożonych reguł korelacyjnych i dashboardów, protokoły z testów oraz procedury administracyjne (aktualizacja – dla sieci OT również w trybie offline,

archiwizacja, kopia zapasowa i odtworzenie konfiguracji). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

6.3.10. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT. Jeżeli w ramach wdrożenia Wykonawca będzie miał dostęp do danych osobowych zawartych w logach, strony zawrą umowę powierzenia przetwarzania danych osobowych.

6.3.11. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

8. Terminy realizacji i odbiór

8.1. Termin dostawy licencji i aktywacji wsparcia producenta: do **20** dni od dnia zawarcia umowy.

8.2. Termin przeprowadzenia szkolenia: do **20** dni od dnia zawarcia umowy, w terminie uzgodnionym z Zamawiającym.

8.3. Termin realizacji wdrożenia: do 14 dni.

8.4. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji oraz potwierdzenia rejestracji wsparcia producenta. Odbiór szkolenia nastąpi na podstawie protokołu odbioru i listy obecności.

8.5. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 6.3.8 oraz przekazaniu dokumentacji z pkt 6.3.9. Po odbiorze wdrożenia w obu sieciach strony podpiszą protokół odbioru końcowego.

9. Rozwiązania równoważne

9.1. Wskazanie w OPZ nazw systemów, usług i źródeł danych, z którymi oferowany system musi współpracować (m.in. AWS, Microsoft Azure, Microsoft Active Directory, Microsoft SQL Server, Oracle, PostgreSQL, MongoDB, Apache Cassandra, InfluxDB, Apache Kafka, MISP, OpenAI, Fireworks, Ollama), wynika z infrastruktury i narzędzi wykorzystywanych lub planowanych przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

9.2. Pozostałe nazwy własne, znaki towarowe, normy i standardy wskazane w OPZ (m.in. MITRE ATT&CK, CIS Benchmark, OpenSCAP, OWASP, PCI DSS, NIST, ISO/IEC 27001) mają charakter przykładowy lub referencyjny. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.