**Załącznik nr 3**

**FORMULARZ SPECYFIKACJI TECHNICZNO-CENOWEJ**

**ZAMAWIANEGO/OFEROWANEGO SYSTEMU**

**Opis techniczny oferowanego przedmiotu zamówienia**

**Uwaga:**

**Wykonawca wpisuje odpowiednio:**

1. **w wierszu „Producent”, nazwę producenta właściwą dla oferowanego systemu odpowiednio,**
2. **w wierszu „Nazwa systemu (oprogramowania lub pakietu oprogramowania)”, nazwę systemu (oprogramowania lub pakietu oprogramowania) właściwą dla oferowanego systemu odpowiednio, jeżeli system/pozycja posiada nazwę wersję/model, numer katalogowy – wykonawca wpisuje te dane w wierszu „wersja/model, numer katalogowy odpowiednio,**
3. **w kolumnie „Spełnienie wymagania”, „TAK” jeżeli zaoferowane rozwiązanie spełnia dane wymaganie, „NIE” jeżeli zaoferowane wymaganie nie spełnia danego wymagania odpowiednio dla każdej pozycji.**

**W przypadku jeżeli choćby w jednej z pozycji wykonawca oświadczył, ż nie spełnia wymagania**

**lub choćby w jednej z pozycji nie oświadczy, że spełnia wymagania będzie uznaniem przez Zamawiającego, że wykonawca nie zaoferował spełnienia wymagania i spowoduje, że oferta zostanie odrzucona jako niezgodna z warunkami zamówienia**

|  |
| --- |
| 1. **System analizy logów i zdarzeń typu Security Information and Event Management**
 |
| Producent |  |
| Nazwa systemu (oprogramowania lub pakietu oprogramowania) |  |
| wersja/model, numer katalogowy |  |

**Szczegółowe parametry systemu typu SIEM**

|  |  |  |  |
| --- | --- | --- | --- |
| Poz. | Wymagania/parametry | Wymagania minimalne(charakterystyka) | Spełnia wymaganie[TAK/NIE] |
| 1 | 2 | 3 | 4 |
| 1 | Wymagania ogólne dla kolektorów systemu | * 1. Wszystkie elementy odpowiedzialne za zbieranie informacji, od tego miejsca określane jako Kolektory, mogą być dostarczone tylko w postaci rozwiązań wirtualnych.
	2. Zadaniem kolektorów jest przesyłanie monitorowanych danych (np. zdarzeń) do warstwy je przechowującej i korelującej
	3. W wypadku awarii komunikacji pomiędzy kolektorami a warstwą przechowującą i korelującą kolektory mają możliwość buforowania otrzymanych informacji oraz istnieje możliwość definiowania rozmiaru bufora dla zdarzeń otrzymywanych przez kolektor oraz monitorowania jego zajętości
	4. Kolektory muszą mieć możliwość ograniczenia ilości zdarzeń przesyłanych do klastra SIEM
	5. Kolektory muszą mieć możliwość kompresowania danych przesyłanych do warstwy przechowującej i korelującej
	6. Kolektory muszą mieć możliwość ograniczania przepustowości z którą zdarzenia są przesyłane do warstwy przechowującej i korelującej
	7. Komunikacja pomiędzy warstwą przechowującą i korelującą musi odbywać się z wykorzystaniem protokołu HTTPS. Odbywa się ona w kierunku od kolektorów do warstwy przechowującej i korelującej dla przesyłanych zdarzeń
	8. W wypadku awarii kolektora, kolektor zastępczy może być uruchomiony poprzez jego zarejestrowanie w warstwie przechowującej i korelującej. Konfiguracja (zarządzanie) kolektorów nie odbywa się indywidualnie lecz są one centralnie zarządzane. Nie mogą one posiadać żadnych parametrów konfiguracyjnych poza adresami IP, nazwą kolektora oraz, wymaganymi poświadczeniami, które byłyby wymagane w celu uruchomienia kolektora zastępczego
	9. Wydajność kolektora nie może być mniejsza niż 3 000 EPS
	10. Kolektory muszą być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu NetFlow
	11. Poszczególne kolektory muszą być w stanie automatycznie aktualizować parsery gdy zostaną one zaktualizowane w centralnym systemie zarządzającym rozwiązaniem SIEM
	12. Kolektory mają mieć możliwość aktualizacji wersji swojego oprogramowania z warstwy zarządzającej
	13. Rozwiązanie SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń
 |  |
| 2 | Warstwa przechowująca i korelująca – klaster SIEM | 1. Implementacja ma być zrealizowana w oparciu o maszyny wirtualne (VA - Virtual Appliance)
2. Możliwość stworzenia architektury redundantnej w której podstawowa instalacja rozwiązania SIEM podczas regularnej pracy wykonuje wszystkie operacje produkcyjne, zaś instalacja backupowa synchronizuje wszystkie dane i w razie awarii jest w stanie przejąć funkcjonowanie środowiska SIEM (konfiguracja active-passive)
3. Możliwość instalacji rozwiązania na następujących platformach wirtualizacyjnych:
	* + VMWare vSphere
		+ Hyper-V
		+ AWS
		+ Azure
4. Możliwość skalowania klastra SIEM poprzez dodawanie kolejnych maszyn wirtualnych (Virtual Appliance - VA). Wspomniana skalowalność ma być realizowana przez:
* przeprowadzaną w czasie rzeczywistym, w pamięci rozwiązania, dystrybucję reguł korelacyjnych,
* dystrybuowanie pomiędzy elementy klastra SIEM zadań raportowania oraz analizy danych.

Mechanizm dystrybucji musi być całkowicie przezroczysty z perspektywy użytkownika, tak aby nie musiał on decydować który z elementów ma być odpowiedzialny za wykonanie poszczególnych zadań.1. Klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej
2. Klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)
3. Dane zbieranych zdarzeń (events) mogą być gromadzone na dyskach maszyn wirtualnych podczas działania w oparciu o pojedynczą maszynę wirtualną lub też z możliwością wykorzystania NFS w sytuacji pracy w trybie klastra SIEM (wiele maszyn wirtualnych).
4. Klaster SIEM musi mieć możliwość obsłużenia (potencjalną możliwość docelowego skalowania do) nie mniej niż 500 tys. EPS.
5. Klaster SIEM musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych/znormalizowanych danych (parsed event log)
6. Rozwiązanie SIEM nie może wymagać zastosowania dodatkowej przestrzeni dyskowej i/lub warstwy służącej do filtrowania lub wysyłania podzbiorów danych przesyłanych od kolektorów do warstwy korelującej
7. Zebrane dane muszą być przechowywane w formie skompresowanej
8. System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji.
9. Klaster SIEM do przechowywania danych związanych ze zbieranymi zdarzeniami wykorzystuje bazę typu noSQL
10. Relacyjne bazy danych mogą być wykorzystywane do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji
11. Maszyny wirtualne systemu SIEM mają działać w oparciu o system Linux który ma mieć możliwość aktualizacji.
 |  |
| 3 | Kolekcjonowanie danych | 1. Możliwość aktywnego wykrywania urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak:
* SNMP
* Syslog
* Windows Management Instrumentation (WMI) and Open Management Infrastructure (OMI)
* Microsoft RPC
* Cisco SDEE
* Checkpoint LEA
* JDBC
* VMware VI-SDK
* JMX
* Telnet
* SSH
* NetFlow
* HTTPS
* IMAP i IMAP over SSL
* POP3
* Kafka API
* import z pliku CSV
* import z pliku PCAP
1. Zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP, TCP, UDP, ICMP, JDBC, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS.

Wyniki powyższego monitoringu mają dawać możliwość obliczenia poziomu dostępności danej usługi (np. procentowego)1. Wykryte urządzenie ma posiadać swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB) w ramach dostarczonego rozwiązania SIEM co jednocześnie ma umożliwiać prezentację następujących informacji (nie mniej niż):
* wersja oprogramowania/firmware/systemu operacyjnego
* numer seryjny urządzenia
* skonfigurowane interfejsy wraz z:
1. nazwą interfejsu
2. adresem IP oraz podsiecią
3. statusem interfejsu (włączony, wyłączony)
4. informacją o skonfigurowanym poziomie bezpieczeństwa
5. prędkością interfejsu
6. możliwością edycji nazwy oraz prędkości interfejsu
* procesach działających na urządzeniu lub systemie operacyjnym
* alarmach w przypadku zmiany statusu procesu np. jego uruchomienia lub zatrzymania
1. Możliwość automatycznego przypisania do grupy poszczególnych urządzeń znajdujących się w CMDB, np. grupa serwerów Windows, grupa rozwiązań firewall, etc.
2. Automatyczne wykrywanie aplikacji działających na poszczególnych urządzeniach. Wymagane jest aby baza urządzeń (CMDB) miała możliwość konfiguracji grup aplikacji celem automatycznego umieszczania w nich poszczególnych urządzeń, np. grupa aplikacyjna "IIS Servers" wyświetla wszystkie urządzenia z uruchomionymi usługami Microsoft IIS
3. Wymagane jest aby rozwiązanie SIEM posiadało wbudowany szablon (template), który po przeprowadzeniu aktywnego wykrywania urządzeń będzie pozwalał na automatyczne określenie jakiego rodzaju dane będą z nich zbierane oraz jaki będzie interwał ich pobierania
4. Monitorowanie następujących metryk wydajnościowych:
* utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych,
* obciążenia procesorów,
* wykorzystania pamięci,
* wykorzystania przestrzeni dyskowej,
* utylizacji poszczególnych procesów.
 |  |
| 4 | Analityka i parsowanie | 1. Rozwiązanie SIEM musi dostarczać zunifikowane narzędzia analityczne dzięki którym możliwe jest wykonywanie zapytań w oparciu o ten sam język zarówno dla logów/zdarzeń zbieranych z urządzeń jak i dla danych wydajnościowych.
2. Wymagane jest aby kolektory systemu SIEM pozwalały na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.
3. Zarówno dane w stanie surowym jak i ten sparsowane lub wzbogacone muszą być możliwe do przesłania do rozwiązania SIEM z kolektorów.
4. Przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe.
5. Możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów
6. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
7. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
8. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:
	1. możliwość do definiowania wzorców które powtarzają się jako zmienne
	2. możliwość dodefiniowania funkcji pozwalających na identyfikację par wartości kluczowych
	3. możliwość przekształcania danych w trakcie ich parsowania
 |  |
| 5 | Monitorowanie | 1. Musi istnieć możliwość monitorowania urządzeń bez wykorzystania aplikacji typu agent poprzez SSH, telnet, WMI, JMX oraz PowerShell
2. Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu aplikacje typu agent
3. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają następujące możliwości:
	* centralne zarządzanie z głównej konsoli systemu SIEM
	* możliwość zbierania logów z plików tekstowych
	* możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application
	* możliwość monitorowania integralności plików
	* możliwość monitorowania rejestru
	* możliwość monitorowania urządzeń zewnętrznych (removable devices)
	* możliwość wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów
	* możliwość wykonywania poleceń WMI wraz z odsyłaniem wyniku ich działania w postaci logów
	* agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokolu HTTPS
	* możliwość monitorowania stanu agentów w konsoli zarządzającej systemu
4. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają następujące możliwości:
	* centralne zarządzanie z głównej konsoli systemu SIEM
	* możliwość zbierania logów z wykorzystaniem protokołu syslog
	* możliwość zbierania logów z plików tekstowych
	* możliwość monitorowania integralności plików
	* możliwość monitorowania pliku w oparciu o jego sumę kontrolną
	* musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu
5. System SIEM musi mieć możliwość relizacji funkcjonalności UEBA (User Entity Behaviour Analysis) w oparciu o dedykowanego Agenta na systemy Windows
 |  |
| 6 | Zarządzanie | 1. System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI
2. System SIEM musi być w stanie wykryć usługi Active Directory oraz LDAP oraz wyświetlać informacje o strukturze katalogowej drzewa w GUI
3. Możliwość wykorzystania struktury katalogowej drzewa LDAP jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych
4. Zewnętrzne metody uwierzytelniania użytkowników SIEM:
	* Active Directory lub LDAP
	* RADIUS
	* SAML
 |  |
| 7 | Bazy informacji o zagrożeniach | 1. Integracja z zewnętrznymi bazami informacji o zagrożeniach (Threat Inteligence feeds - TI):
	* wsparcie dla plików CSV musi być wykonywalne z wykorzystaniem interfejsu graficznego GUI
	* definicje w ramach integracji muszą zawierać nie mniej niż:
		1. adresy IP
		2. domeny
		3. sumy kontrolne (hash)
		4. adresy URL
	* wymagane jest aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tys. wpisów
	* wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw komercyjnych baz zagrożeń
	* wraz z systemem SIEM musi być wspierany, już zintegrowany, zestaw baz zagrożeń niekomercyjnych (open source)
	* system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data)
	* system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
	* system musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal,
	* system musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK w oparciu o wbudowane reguły, których ilość w tym kontekście ma wynosić nie mniej niż 900
 |  |
| 8 | Raporty | 1. System SIEM musi mieć możliwość analizowania i odpytywania o zdarzenia w widoku analitycznym w trybie strumieniowym (streaming mode), w taki sposób że raport docelowy dotyczący analizowanych zdarzeń wykonywany jest przed ich zapisaniem na dysk twardy
2. Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów:
	* PCI-DSS
	* HIPAA
	* SOX
	* NERC
	* FISMA
	* ISO
	* GLBA
	* GPG13
	* SANS Critical Controls
 |  |
| 9 | Pulpit administracyjny | 1. System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML
2. System SIEM musi pozwalać na zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji obok siebie
3. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji
4. Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji:
	* Bar
	* Pie
	* Line
	* Table
	* Combination (line and table view)
	* Treemap
	* Scatter graph
	* Single values
	* Gauges
	* Geographical Map
 |  |
| 10 | Powiadomienia oraz zarządzanie incydentami | System SIEM musi:1. posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach,
2. posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty,
3. możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty musi być możliwa w oparciu o role z podziałem na użytkowników mających pełne prawa do uruchamiania skryptów i na użytkowników zgłaszających żądanie uruchomienia skryptu, które to żądanie musi być zatwierdzone przez użytkownika nadrzędnego,
4. mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system).
 |  |
| 11 | Analityka | * + - 1. System SIEM musi mieć możliwość:
* wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów
* zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN
* wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych
* wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.
* wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem
* wyszukiwania w oparciu o nie mniej niż następujące operatory: include, =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex
* podejmowania w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń
* w przypadku prostych zapytań musi na przykład być możliwe określenie wartości granicznej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z Z wybranych wartości
* w przypadku zapytań przekrojowych wspierających filtry typu Boolean musi być możliwe:
1. stworzenie wzorców zapytań za określony przedział czasu z wykorzystaniem operatorów takich jak: AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED BY
2. każdy z wzorców może być filtrowany i agregowany z wykorzystaniem operatorów takich jak: AVG, MAX, MIN, COUNT and COUNT DISTINCT
3. ustalane wartości graniczne (thresholds) mogą być statyczne lub też mogą być otrzymywane jako rezultat analizy statystycznej
* analiza statystyczna i alarmowanie w oparciu o zdarzenia musi mieć możliwość działania w oparciu o:
1. średnie kroczące (moving averages)
2. odchylenia standardowe (standard deviations)
* w wypadku przekroczenia statystycznej wartości granicznej (statistical threshold) musi zostać wygenerowany alert w czasie zbliżonym do rzeczywistego
* wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenie reguł
* tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną
* możliwości eksportowania raportów do formatów CSV i PDF
* wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego
* wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej
* skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM
* automatycznego korelowania użytkownika z jego lokalizacją i adresem IP:
* musi istnieć możliwość tworzenia raportów i wyszukiwania użytkownika w połączeniu z jego adresem IP oraz lokalizacją. Lokalizacja może oznaczać port na switch'u, adres MAC lub połączenie VPN
* musi istnieć możliwość wzbogacania zdarzeń (events) przy których dane użytkownika pozbawione są informacje o adresie IP
* wykorzystanie funkcjonalności Geo IP w oparciu o bazę pochodzącą od tego samego producenta
* możliwość wykrywania zdarzeń IPS false positive w oparciu o integrację z zewnętrznymi skanerami podatności
1. System SIEM musi pozwalać na przesłanie dowolnych zebranych zdarzeń z wykorzystaniem protokołu KAFKA
 |  |
| 12 | Archiwizacja i integralność danych | 1. System SIEM musi pozwalać na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS.
2. Integralność danych związanych ze zdarzeniami musi być weryfikowalna z wykorzystaniem GUI w oparciu o przeliczenie sum kontrolnych, które obliczane były w momencie zapisywania danych o zdarzeniach na dysk systemu SIEM
3. System musi mieć możliwość uruchomienia w trybie zgodności z FIPS
 |  |
| 13 | Wsparcie | * + - 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.
 |  |
| 14 | Wymagania licencyjne | 1. Licencja zapewniająca zbieranie informacji z co najmniej 300 urządzeń w tym minimum 300 dedykowanych agentów dla systemów Windows lub Linux oraz 3000 EPS. Model licencyjny musi umożliwiać zwiększanie ilości urządzeń i EPS poprzez zakup dodatkowych subskrypcji lub ich rozszerzeń w dowolnym czasie.
2. Oprogramowanie musi być dostarczone w modelu „na własność” tj. niewykupienie licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania urządzenia a jedynie pozbawi możliwości pobierania aktualizacji systemu.
 |  |

**Cena netto:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**VAT 23%**

**Cena brutto: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**