Załącznik nr 1 – Specyfikacja oprogramowania SIEM

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja systemu do gromadzenia i zarządzania logami (Logserwera) oraz systemu typu SIEM w celu centralizacji, analizy i monitorowania logów z różnych źródeł w formie licencji wieczystej ze wsparciem na okres 1 roku od podpisania protokołu odbioru systemu.

2. Wymagania SIEM

2.1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2.2. System musi pracować w oparciu o architekturę Linux.
2.3. System musi mieć możliwość centralnego zbierania i zarządzania logami
2.4. System działać w trybie zbliżonym do rzeczywistego
2.5. System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet
2.6. System musi mieć możliwość działania jako niezależne instancje zainstalowane w jednostkach Zamawiającego wraz z możliwość centralnego dostępu.
2.7. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
2.8. System musi zapewniać efektywną obsługę do 20 GB danych dziennie
2.9. System musi zapewniać retencję danych w okresie minimum 120 dni.
2.10. Oferowany system nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
2.11. Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
2.12. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
2.13. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
2.14. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
2.15. Interfejs musi posiadać angielską lub polską wersję językową.
2.16. System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
2.17. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
2.18. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
2.19. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
2.20. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
2.21. System musi pozwalać na tworzenie parserów z poziomu GUI

2.22. System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
2.23. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
2.24. System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
2.25. Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie 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).
2.26. Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.
2.27. 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, aby izolowane zdarzenia można było łatwo zidentyfikować.
2.28. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
2.29. Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
2.30. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
2.31. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
2.32. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
2.33. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
2.34. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
2.35. System musi zapewniać parsowanie spływających do niego wiadomości w formatach: Syslog, WEF, Flat file, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC, CSV, Email, jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
2.36. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
2.37. System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB, Firebird, SQL Anywhere i Apache Kafka
2.38. 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.
2.39. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.

2.40. Operacja z rekordami bazy danych musza być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.
2.41. Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.
2.42. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
2.43. Interfejs musi umożliwić 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.
2.44. System musi posiadać predefiniowany zestaw parserów zdarzeń.
2.45. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta.
2.46. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
2.47. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
2.48. System musi umożliwiać przeszukiwanie danych wejściowych z uwzględnieniem filtracji po sparsowanych polach.
2.49. Proces parsowania musi umożliwiać wzbogacanie treści obieranych wiadomości poprzez matematyczne operacje wykonywane na innych polach.
2.50. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
2.51. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
2.52. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
2.53. 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.
2.54. Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
2.55. System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.
2.56. System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
2.57. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
2.58. System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL oraz Piped Processing Language (PPL).
2.59. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
2.60. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.

2.61. 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 w wskazany sposób względem czasu poprzedniego,
- wykrycia zaniku Wiadomości,
- wykrycia nowej wartości pola w zadanym okresie czasu,
- wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności

2.62. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów

2.63. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.

2.64. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.

2.65. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.

2.66. System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności

2.67. System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, w tym minimum protokołów HTTP DNS, FTP oraz SSH.

2.68. System na bazie gromadzonej kopii ruchu sieciowego musi identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników.

2.69. System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP.

2.70. System musi umożliwiać gromadzenie i analizowanie danych Netflow, w tym: IPFIX, sFlow, J-Flow, Netflow v9.

2.71. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.

2.72. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook

2.73. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

2.74. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

2.75. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).

2.76. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.

2.77. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
2.78. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
2.79. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
2.80. System musi posiadać wbudowany, dostępny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
2.81. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 1 roku.
2.82. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
2.83. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
2.84. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.
2.85. Support producenta musi być świadczony w formule minimum 8/5.
2.86. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.
2.87. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.

Zamawiający oczekuje, że Wykonawca wraz z licencją produkcyjną Wykonawca zobligowany jest dostarczyć licencję na potrzeby środowiska testowego, która umożliwi przetwarzanie minimum 1 000 EPS.

Licencja testowa musi być objęta supportem producenta na takich samych zasadach jak licencja produkcyjna.

3. Dostęp do systemu

Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.

Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokół TLS w wersji minimum 1.3.

System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.

Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.

Autoryzacja do systemu musi mieć możliwość integracji z: Microsoft AD, LDAP, Radius

Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.

System musi wspierać mechanizm logowania typu Single Sign On.

System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.

System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.

System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.

4. **Przyjmowanie, identyfikacja i wizualizacja danych**

Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.

System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.

System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.

System posiada natywną integrację z Mitre ATT@CK.

5. **Reguły korelacyjne, alerty i obsługa incydentów**

System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych

System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.

System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.

System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST, ISO 27001

System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów

System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows

System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

6. **Raportowanie i Archiwizacja danych**

System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.

Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.

Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.

Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.

System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.

Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.

System musi generować raporty do formatów minimum PDF, docx oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.

7. Lista źródeł

Źródłami danych będą serwery Windows, Linux, stacje robocze Windows, UTM Fortigate oraz Barracuda, router OpnSense, system NAC – NACVIEW, switche Cisco, DCN, Netgear, dysk sieciowy QNAP