



## Opis przedmiotu zamówienia

**Oprogramowanie klasy SIEM umożliwiające centralizację składowanie i analityki zdarzeń pochodzących ze wszystkich możliwych obszarów IT wyposażone w mechanizmy automatycznej korelacji logów wykrywa – licencja wieczysta z wdrożeniem i 2 lata gwarancji.**

### Wymagania funkcjonalne

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.- lub równoważną
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu.
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 5000 EPS lub 100 GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365 dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer. – lub równoważne



18. Interfejs musi posiadać angielską lub polską wersję językową.
19. System powinien 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). – lub równoważne
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius – lub równoważne
22. Hasła typu Windows AD bind – lub równoważne, muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. System powinien umożliwiać zarządzanie 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.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
31. System musi pozwalać na tworzenie parserów z poziomu GUI
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.



**37.** 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.

- 38.** System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure. – lub równoważne
- 39.** 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.
- 40.** System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
- 41.** System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
- 42.** 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 lub równoważne oraz umożliwiać zastosowanie innego parsera.
- 43.** System musi posiadać predefiniowany zestaw parserów zdarzeń.
- 44.** System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
- 45.** System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
- 46.** 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.
- 47.** System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
- 48.** Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
- 49.** Proces parsowania musi umożliwiać anonimizację danych wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.



50. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
51. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
52. 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.
53. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
54. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
55. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
  - a. Wykrycia dowolnej treści w logach,
  - b. Wykrycia wystąpienia wartości pola na wybranej liście,
  - c. Wykrycia niewystępowania wartości pola na wybranej liście,
  - d. Wykrycia zmiany jednego z kilku pól,
  - e. Wykrycia zdarzeń występujących z zadaną częstotliwością,
  - f. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
  - g. Wykrycia zaniku Wiadomości,
  - h. Wykrycia nowej wartości pola w zadanym okresie czasu,
  - i. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
56. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
57. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
58. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
59. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
60. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
61. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
62. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
63. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.



64. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
65. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
66. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
67. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
68. 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.
69. System umożliwia konfigurację automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
70. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
71. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
72. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
73. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
74. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
75. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
76. Mechanizm archiwizacji musi umożliwiać pozwalając na przywracanie danych do systemu celem analizy online.
77. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
78. System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizy formatu Netflow w wersji min. V5, v9 oraz IPFIX z wykorzystaniem oficjalnych modułów dostarczanych przez producenta. – lub równoważne
79. System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, retransmisji, Jitter, Server Response Time oraz Round Trip Time.
80. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 2 lat.



81. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
82. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
83. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.
84. Support producenta musi być świadczony w formule minimum 8/5.
85. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.
86. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
87. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
88. System musi umożliwiać integrację z Mitre ATT@CK. – lub równoważne
89. Reguły korelacyjne, alerty i obsługa incydentów
90. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
91. 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.
92. 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.
93. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
94. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
95. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
96. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP – lub równoważne

## **Szkolenia**

1. Wykonawca dostarczy voucher szkoleniowy dla 2-óch słuchaczy dla systemu SIEM.
2. Szkolenie odbędzie się w formie zdalnej.
3. Szkolenie musi być prowadzone w języku polskim.
4. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



5. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.
6. Opracowanie harmonogramu wdrożenia systemu SIEM.
7. Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.
8. Przeprowadzenie instalacji i konfiguracji systemu SIEM.
9. Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.
10. Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboards z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
11. Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.
12. Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
13. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
14. Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.
15. Support producenta musi być świadczony w formule minimum 8/5. Wymagane oświadczenie producenta potwierdzające dostępność inżynierów w trybie 8/5.
16. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedziby Zamawiającego.
17. Producent systemu SIEM musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnić gotową integrację z systemem SOAR tego samego producenta.