Szczegółowy opis przedmiotu zamówienia

I. Opis posiadanych przez Zamawiającego licencji, wsparcia dla posiadanego systemu SIEM oraz infrastruktury

1. Licencja Splunk Enterprise Security 60GB/day (Splunk Enterprise Term License - No Enforcement (6.5)), ze wsparciem producenta ważna do dnia 24.12.2023 r.
2. Licencja Splunk Enterprise 60GB/day (Splunk Enterprise Term License - No Enforcement (6.5)), ze wsparciem producenta ważna do dnia 24.12.2023 r.
3. Zamawiający obecnie wykorzystuje oprogramowanie do wirtualizacji vSphere7 Essential Plus Kit (dla 3 hostów) oraz Veeam Backup and Replication (licencjonowany dla 6 CPU) do tworzenia kopii środowiska. Datastore dla środowiska wirtualizacyjnego są udostępniane bezpośrednio z macierzy poprzez iSCSI (10gbe).
4. Zamawiający posiada uruchomione następujące maszyny wirtualne dla w/w rozwiązania:
   1) Splunk MC, DS Lic Srv,
   2) Splunk Heavy Forwarder #1,
   3) Splunk Heavy Forwarder #2
   4) Splunk - Indexer #1,
   5) Splunk - Indexer #2,
   6) Splunk – Search Head #1
   7) Splunk – Search Head #2

II. Przedmiot zamówienia

Przedłużenie licencji dla posiadanego systemu SIEM opartego na architekturze Splunk Enterprise wraz z usługą serwisu i wsparcia technicznego producenta na poziomie Standard, z okresem obowiązywania od dnia 25.12.2023 r. na okres obowiązywania umowy, tj. 18, 24 lub 36 miesięcy, w modelu tradycyjnym (on-premise) na istniejącej infrastrukturze Zamawiającego.

Zamawiający dopuszcza dostarczenie oprogramowania równoważnego spełniającego wymagania określone w pkt III SOPZ.

III. Opis wymagań dla oprogramowania równoważnego

A. Wymagane funkcjonalności systemu SIEM (dalej jako: „System”):

1. Oferowany System musi być rozwiązaniem komercyjnym, posiadającym wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source.
2. Oferowany System musi funkcjonować w środowisku wirtualizacyjnym VMware.
3. Zamawiający nie dopuszcza rozwiązań chmurowych.

4. Oferowane funkcjonalności muszą mieć pokrycie w oficjalnie dostępnej dokumentacji technicznej producenta, którą dostawca udostępni na żądanie Zamawiającego wraz ze wskazaniem punktów odnoszących się do danej funkcjonalności wymaganej w OPZ.
5. System musi cechować się uniwersalnością, tzn. oprócz funkcjonalności dedykowanych bezpieczeństwu powinno zapewniać możliwość wykorzystania wybranego rozwiązania do analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych.
6. Rozwiązanie musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami Systemu.
7. System musi samodzielnie zarządzać retencją danych.
8. System musi umożliwiać na konfigurację w wysokiej dostępności eliminującej wystąpienie pojedynczego punktu awarii.
9. Architektura Systemu musi umożliwiać na rozdzielenie na osobne komponenty (w domyśle maszyny wirtualne) funkcji związanych z pobieraniem danych, przechowywaniem, wyszukiwaniem i zarządzaniem zebranymi logami.
10. System nie może posiadać ograniczeń w postaci ilości urządzeń, z których pobierane są logi, jak również liczby źródeł generowanych logów;
11. System musi zapewniać wydajność parsowania logów, których wielkość dochodzi do 60/70/101 GB dziennie oraz dla których częstość zdarzeń na sekundę (EPS) może dochodzić do 36000 EPS;
12. System nie może blokować/odrzucać logów/danych w przypadku przekroczenia dziennego limitu danych (w odniesieniu do wykorzystywanych w danym momencie licencji), jak również otrzymywanych zdarzeń na sekundę (EPS);
13. System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę na co najmniej 15TB danych;
14. System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych;
15. System musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (surowej - raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwe w oparciu o te same narzędzia;
16. Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól;

17. System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne;
18. Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje: Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego); Funkcje wykrywania anomalii danych liczbowych. Rozwiązanie musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach a nie tylko parametrów ruchu sieciowego; System musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze; Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól; Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).
19. System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności, związanych z analizą danych obejmującą:
    1) mechanizmy pobierania danych,
    2) raporty, dashboardy i formularze,
    3) nowe funkcje analityczne,
    4) nowe sposoby wizualizacji,
    5) mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent.

    Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta.
20. Musi istnieć możliwość tworzenia interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie, jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenie ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych);
21. System musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem: tabel, wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), map, map kolorowanych. Tworzenie wyżej wymienionych komponentów wizualizacji musi odbywać się bezpośrednio na poziomie zapytania.
22. System musi umożliwiać integrację danych gromadzonych z różnych źródeł: aplikacji, baz użytkowników, w tym katalogu Active Directory. Dane muszą być dostępne jako spójna informacja na poziomie interfejsu analitycznego systemu;
23. Komunikacja użytkownika z Systemem musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Microsoft Edge, Firefox, Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników, w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight;

24. System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck).
25. System musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji Systemu.
26. Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi, takich klient SSH lub RDP;
27. System musi wspierać Role Based Access Control (RBAC), umożliwiając precyzyjne nadawanie uprawnień dla administratorów, w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania co najmniej LDAP lub Active Directory;
28. Zaoferowany System musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych) jak również w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów: Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog); Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay; Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog. Wykonywanie zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC; Windows Management Infrastructure (WMI).
29. System musi umożliwiać pobieranie logów z co najmniej następującymi protokołami:
    1) syslog UDP/TCP,
    2) trap SNMP,
    3) logi i informacje przechowywane w bazach danych. Nie mniej niż Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie),
    4) pliki tekstowe,
    5) WMI,
    6) NetFlow v5 i v9, sFlow, jFlow, IPFIX.

    Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.
30. System musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na

którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie. Agent musi zapewniać możliwość szyfrowania i uwierzytelniania komunikacji z serwerem centralnym. Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązań działających w klastrze lub niezależnie;

31. System musi posiadać interfejs programowania aplikacji (API) w postaci bibliotek programistycznych dla języków: Java, Python, JavaScript, PHP, Ruby oraz C#;
32. System musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów:
    1) DHCP,
    2) DNS,
    3) HTTP,
    4) IMAP,
    5) SIP,
    6) SMB,
    7) SMTP.

    Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze;
33. System musi posiadać udokumentowany interfejs REST (Representational State Transfer) umożliwiający integrację z zewnętrznymi systemami teleinformatycznymi;
34. Mechanizm przechowywania logów/danych/zdarzeń Systemu musi uniemożliwiać nieupoważnione usunięcie całości lub części logów, danych, raportów i innych informacji oraz zapewniać dostęp do nich tylko dla uprawnionych, uwierzytelnionych użytkowników;
35. Przechowywane dane muszą być zabezpieczone przed modyfikacją przy wykorzystaniu metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem;
36. System musi umożliwiać Zamawiającemu skalowalność/rozbudowę architektury/infrastruktury w przypadku wzrostu wymagań wydajnościowych i pojemnościowych wynikających z przekazywania, gromadzenia oraz zwiększania szczegółowości poziomu logowanych zdarzeń (logów/danych);
37. System musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów klastra w celu spełnienia wymagań dot. wydajności lub dostępności.

38. Rozwiązanie musi wspierać mechanizm planowanego przenoszenia danych na pamięci masowe niższego poziomu na podstawie czasu lub okresu.
39. System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line.
40. Licencja Systemu nie może ograniczać liczby elementów gromadzących oraz analizujących logi;
41. Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http_user_agent) oraz opcjonalnie agregacji danych;
42. System musi zapewnić nieprzerwaną kontynuację pracy w przypadku awarii jednego z centrum przetwarzania danych lub dowolnego elementu infrastruktury tego Systemu;
43. System musi posiadać oraz umożliwiać akceleracje często wykonywanych zapytań i raportów, tak aby automatycznie przyśpieszać wykonanie raportu obejmującego długie okresy czasu (np. 6 miesięcy). Akceleracja musi być dostępna zarówno dla raportów wbudowanych, jak i własnych definiowanych przez użytkownika;
44. Tabele i wykresy prezentowane na bazie dostarczonych logów/danych muszą posiadać funkcję drill-down, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie interfejs musi pokazywać odpowiadające im logi/dane;
45. Musi istnieć możliwość definiowania akcji typu drill down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje muszą obejmować zewnętrzny URL lub raport/dashboard w samym Systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól, których dotyczy akcja drilldown;
46. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do Systemu;
47. System musi automatycznie (tj. bez uprzedniego definiowania schematu danych wejściowych) analizować dane zdarzenie (dzienniki systemowe, w szczególności w formie Syslog, Netflow) pod kątem zawartości i struktury danych. Wynikiem analizy muszą być informacje mapowane w formacie łatwym do późniejszego wyszukiwania i analizy, np. w strukturach klucz-wartość;
48. System musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne (np. kraj) dla zdarzeń mają służyć w narzędziu do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych;
49. System musi umożliwiać analizę standardowych logów infrastrukturalnych – generowanych przez systemy operacyjne, dostęp webowy, firewalle, urządzenia sieciowe (switche, routery,

loadbalancery itd.), systemy bezpieczeństwa IPS/IDS/ Application & URL Filtering/Anti-Bot, WAF, IDM, DAM, itd.;

50. Mechanizm pobierania logów/danych ze źródeł, musi umożliwiać wstępną selekcję logów/danych przed wysłaniem ich do Systemu oraz/lub rozpoczęciem parsowania (bez konieczności rekonfiguracji poziomu logowania zdarzeń w źródle), w celu analizy tylko istotnych zdarzeń, jak również oszczędności wynikających z ograniczeń licencyjnych i wydajnościowych;
51. System musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji;
52. System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.);
53. System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól muszą być określone strukturą XML. System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól muszą być określone strukturą JSON;
54. System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól muszą być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach;
55. System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość, np. „user=jkowalski” musi tworzyć pole „user” o wartości „jkowalski”;
56. System musi umożliwiać obsługę logów w formacie CEF, JSON i CSV
57. Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach:
    1) Katalogi LDAP,
    2) Bazy danych,
    3) Bazy noSQL
    4) Dane geolokalizacyjne.
58. W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami a wzbogacanie musi odbywać w locie w trakcie odczytu danych ze źródeł zewnętrznych.
59. System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót;
60. System musi umożliwiać wydajną pracę użytkownika przeglądającego zdarzenia i generującego raporty oraz samego Systemu, w szczególność parsowania danych, których wielkość dochodzi do 60/70/101 GB dziennie;

61. System musi umożliwiać parsowanie logów o długości co najmniej 10000 znaków oraz zawierających więcej niż jedna linię;
62. System musi umożliwiać tworzenie bazy definicji formatów logów;
63. Proces odpowiedzialny za parsowania logów musi analizować poszczególne logi/dane, i wyszukiwać w nich istotne informacje o logowanym zdarzeniu, między innymi: data i czas zdarzenia, nazwa użytkownika, nazwa systemu logującego, nazwa/adres IP systemu, źródła logów, rodzaj zdarzenia (np. zalogowanie/ wylogowanie/zablokowanie użytkownika, przepuszczenie/zablokowanie ruchu sieciowego, wykrycie szkodliwego kodu itp.);
64. System musi automatycznie proponować definicje pól, dla poszczególnego typu logów wykorzystywanych do dalszej analizy oraz tworzyć statystyki występowania poszczególnych wartości tych pól;
65. System musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych;
66. System musi umożliwiać definiowanie pól za pomocą wyrażeń regularnych (REGEX);
67. System musi umożliwiać w czasie rzeczywistym wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX);
68. System musi umożliwiać przeglądanie (w jednej konsoli systemu) w czasie rzeczywistym, logów pobieranych/dostarczanych do Systemu w celu uniknięcia konieczności logowania się do każdego monitorowanego systemu osobno, w celu sprawdzenia statusu połączenia (przepuszczone, zablokowane). Filtrowanie w czasie rzeczywistym musi dopuszczać wyszukiwanie informacji za pomocą wyrażeń regularnych (REGEX);
69. System musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną;
70. System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł;
71. System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danej Systemu; Zamawiający nie dopuszcza Systemy, w którym do tworzenia reguł korelacyjnych przy użyciu dodatkowych narzędzi firm trzecich
72. Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).
73. System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze

sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w Systemie;

74. Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości;
75. System musi umożliwiać wykrywanie sytuacji niestandardowej (anomalii) niezgodnej z poprzednio zarejestrowanym wzorcem (np. w celu wykrycia ataku DOS, wykrycia wewnętrznego ruchu sieciowego który wcześniej nie występował, uruchomienia nowej niewystępującej wcześniej aplikacji, pojawienia się nowego użytkownika itp);
76. W Systemie musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów wiadomością e-mail, w postaci PDF;
77. System musi wspierać pracę użytkowników o różnych rolach i w następujących obszarach:
    1) Analiza zdarzeń w obszarze bezpieczeństwa teleinformatycznego,
    2) Analiza pracy systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń teleinformatycznych,
    3) Analiza pracy aplikacji wdrażanych/tworzonych przez pracowników NCBR.
78. System musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych;
79. System musi umożliwiać jednoczesną pracę analityczną co najmniej dla 20 użytkowników;
80. Licencja Systemu musi umożliwiać utworzenie kont i pracę dla co najmniej 20 użytkowników;
81. System musi umożliwiać odseparowanie środowiska pracy użytkowników o różnych rolach;
82. System musi być odporny na ataki sieciowe;
83. System musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu;
84. System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:
    1) Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych,
    2) Możliwość przypisania incydentu do osoby,
    3) Możliwość zmiany statusu i priorytetu incydentu,
    4) Możliwość tworzenia komentarzy,
    5) Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy,
    6) Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki,

7) Możliwość raportowania wydajności obsługi incydentów.

B. Zakres wsparcia technicznego producenta Systemu:

1. Dostęp do pomocy technicznej oprogramowania z dostępnością i czasami reakcji
   1) W przypadku gdy oprogramowanie jest całkowicie niedostępne lub większość jego funkcji jest niefunkcjonalna – dostępność 24/7/365 z czasem reakcji 2 godziny.
   2) Jedna lub więcej ważnych funkcjonalności zakupionego oprogramowania stała się niefunkcjonalna lub funkcjonuje błędnie – dostępność 8x5 z czasem reakcji 1 dzień roboczy.
2. Dostęp do poprawek i nowych wersji Systemu;
3. Dostęp do dokumentacji technicznej;
4. Dostęp do konta wsparcia oprogramowania SIEM, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta oprogramowania.

C. Zakres serwisu i wsparcia technicznego świadczonego przez Wykonawcę:

1. Wykonawca zapewni wsparcie techniczne przez okres obowiązywania umowy. Objęcie usługami wsparcia technicznego i serwisu Systemu SIEM musi zapewnić Zamawiającemu pełną gotowość Wykonawcy do świadczenia opisanych w niniejszej specyfikacji usług. Ponadto, świadczone usługi nie mogą negatywnie wpływać na zintegrowane z Systemem SIEM aplikacje biznesowe i inne systemy bezpieczeństwa informacji.
2. Wykonawca w ramach świadczonego wsparcia technicznego zapewni dostępność zespołu składającego się, z co najmniej dwóch inżynierów, posiadających stosowne kompetencje, potwierdzone certyfikatem ukończenia szkolenia z technologii wdrożonego Systemu.
3. Zapewnienie systemu zgłoszeń, dostępnego dla upoważnionych pracowników Zamawiającego, w dni robocze (poniedziałek-piątek) od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy, spełniającego poniższe wymagania:
   1) System zgłoszeń musi obejmować następujące kanały zgłoszeń: serwis WWW, poczta elektroniczna, telefon.
   2) W ramach systemu zgłoszeń zapewnienie kanału WWW do śledzenia i aktualizacji zarejestrowanych zgłoszeń oraz zapewnienie możliwości automatycznego dodawania wpisów w systemie poprzez e-mail.
4. Usuwanie usterek i błędów z zachowaniem poniższych zasad:
   1) Jako błąd krytyczny uznana zostanie sytuacja, z powodu której System nie funkcjonuje lub kiedy nie można wykonać w nim kluczowych czynności.
   2) Za inny błąd uznana zostanie sytuacja, w której System nie funkcjonuje poprawnie tzn. nie można wykonać pewnych czynności w standardowy sposób, ale istnieje możliwość ich wykonania inaczej. Za inny błąd zostanie również uznana sytuacja kiedy z powodu błędu

System przestanie funkcjonować stabilnie lub gdy w sposób znaczny wydajność Systemu zostanie ograniczona.

3) Mianem usterki określone zostanie zdarzenie, w którym uszkodzeniu uległ jeden (lub więcej) element Systemu, nie wpływające na funkcjonalność i wydajność Systemu, ale niezgodne ze stanem określonym w umowie i SOPZ (np. uszkodzenie jednego z elementów zapewniających redundancje Systemu).
4) Usunięcie błędu krytycznego lub wykonanie obejścia błędu krytycznego (umożliwiającego korzystanie z Systemu SIEM) nastąpi w czasie 48h od przekazania zgłoszenia przez Zamawiającego. Jeżeli jednak bezpośrednią przyczyną powstania błędu krytycznego Systemu SIEM jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z producentem Rozwiązania w terminie możliwie najszybszym z punktu widzenia producenta, nie dłuższym niż 2 dni roboczych od przyjęcia zgłoszenia.
5) Usunięcie innych błędów nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
6) Usunięcie usterek nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
7) W przypadku braku możliwości usunięcia usterek i błędów w podanych wyżej terminach, Wykonawca niezwłocznie dostarczy i wdroży czasowo równoważne rozwiązanie zastępcze (workaround). Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego.
8) Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni od daty jego wdrożenia.

D. Świadczenie usługi konsultacyjnej w zakresie funkcjonowania Systemu w ramach prawa opcji:

1. Wymiar: do 350 roboczogodzin;
2. Dostępność: dni robocze od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy;
3. Miejsce: zdalnie;
4. Wsparcie w pracach rozwojowych i zadaniach administracyjnych.

E. Usługa wdrożeniowa

1. Zamawiający na potrzeby wdrożenia w środowisku produkcyjnym udostępni zasoby klastra (3 hosty po dwa CPU 16C) VMware umożliwiające uruchomienie maszyn o sumarycznych parametrach 64 CPU (3,4GHz), 256 GB RAM; 15TB przestrzeni dyskowej SSD oraz 60TB przestrzeni dyskowej HDD.
2. W przypadku większych wymagań systemu równoważnego dla optymalnego działania oferowanego systemu SIEM, Wykonawca zobowiązany jest dostarczyć i zainstalować

niezbędną infrastrukturę we własnym zakresie przy czym dostarczana infrastruktura musi w pełni współpracować z posiadanym i udostępnianym przez Zamawiającego rozwiązaniem opartym o serwery Dell, macierze Dell EMC, środowiskiem wirtualizacyjnym oraz środowiskiem kopii zapasowych oraz spełniać rekomendowane wymagania sprzętowe wskazane przez producenta systemu równoważnego (wymagania te muszą być publicznie dostępne na witrynie producenta), być fabrycznie nowe i wyprodukowane nie wcześniej niż w 2022 roku. Dodatkowe komponenty infrastruktury muszą być w obudowie rack (nie dopuszcza się urządzeń stojących).

3. *(dotyczy dodatkowych komponentów infrastruktury)* Zamawiający udostępni szafę rack (42U) na potrzeby dodatkowego wyposażenia.
4. *(dotyczy dodatkowych komponentów infrastruktury)* Zamawiający nie dostarczy licencji systemów operacyjnych, na których zostanie uruchomione rozwiązanie. Wykonawca musi przewidzieć odpowiednie licencje w ramach składanej oferty.
5. *(dotyczy dodatkowych komponentów infrastruktury)* Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, kable Ethernet kat. 6e, szyny rack, organizery okablowania itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich dodatkowych elementów infrastruktury dostarczanych w ramach przedmiotowego postępowania.
6. Wykonawca w przypadku zaoferowania dodatkowych elementów infrastruktury musi rozszerzyć posiadaną przez Zamawiającego licencje na oprogramowanie do tworzenia kopii zapasowych o dodatkowe elementy infrastruktury. Zamawiający nie pozwala na wymianę oprogramowania do kopii zapasowych.
7. Wykonawca w przypadku zaoferowania dodatkowych elementów infrastruktury musi rozszerzyć posiadaną przez Zamawiającego licencje na oprogramowanie do wirtualizacji o dodatkowe elementy infrastruktury takie jak serwery. Zamawiający nie pozwala na wymianę oprogramowania do wirtualizacji. Zamawiający wymaga, aby oprogramowanie do wirtualizacji (hypervisor ESXi) było zarządzane przez oprogramowanie do zarządzania klastrem (vCenter).
8. Zamawiający planuje uruchomienie Systemu z podłączonymi następującymi źródłami logów:

Rodzaj usługi lub urządzenia	**Liczba urządzeń / nodów będących źródłami logów**
Active Directory (liczba serwerów DC)	6
Windows Server (2012-2022)	120
Linux Server CENTOS / REDHAT / Ubuntu	150
DNS	6
Urządzenia aktywne sieci (przełączniki)	160

Urządzenia aktywne sieci (zapory sieciowe z IPS/IDS i VPN)	8
WAF	2
Dedykowane aplikacje Zamawiającego	4
Systemy bezpieczeństwa (PAM, XDR, Skanery podatności, AV, DLP)	12
Serwery aplikacyjne (IIS, Apache)	50
Serwery bazodanowe (MSSQL, PostgreSQL, MySQL, Maqriadb)	16
SaaS – o365 E5 oraz AAD	1

9. Wdrożenie Systemu równoważnego, w terminie 10 dni kalendarzowych od podpisania umowy, obejmujące w szczególności:
   1) opracowanie Projektu Technicznego wdrożenia dla Środowiska. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. Projekt Techniczny wdrożenia musi zawierać minimum:
      a) Wykaz wykorzystanego sprzętu i licencji oprogramowania.
      b) Przyjęte nazewnictwo elementów infrastruktury.
      c) Plan rozmieszczenia sprzętu w szafie (w przypadku dostawy dodatkowych elementów infrastruktury).
      d) Projekt zarządzania infrastrukturą w serwerowni (w przypadku dostawy dodatkowych elementów infrastruktury).
      e) Projekt konfiguracji infrastruktury wirtualizacji (w przypadku dostawy dodatkowych elementów infrastruktury).
      f) Projekt konfiguracji zasobów dyskowych (w przypadku dostawy dodatkowych elementów infrastruktury).
      g) Projekt instalacji systemów operacyjnych na dostarczonych/udostępnianych serwerach wirtualnych z uwzględnieniem wygenerowania certyfikatów na potrzeby bezpiecznej komunikacji pomiędzy komponentami Systemu oraz użytkowników/operatorów/administratorów Systemu.
      h) Projekt migracji obecnego rozwiązania Zamawiającego i zgromadzonych w nich danych oraz reguł korelacji do rozwiązania wdrażanego w ramach przedmiotowego postępowania. Migracja rozwiązań agentowych służących do przekierowania logów do aktualnie wykorzystywanego systemu dla wszystkich obsługiwanych serwerów.
      i) Projekt konfiguracji infrastruktury sieci LAN oraz dostęp ze wskazanych stacji administracyjnych.
      j) Projekt przekierowania logów do systemu z warstwy hardwarowej oraz warstwy systemów operacyjnych i aplikacji dedykowanych w środowisku Zamawiającego.

k) Projekt uruchomienia dedykowanych dashboardów opartych o zdefiniowane źródła logów dla personelu SOC.

2) wykorzystanie zasobów udostępnionych przez Zamawiającego oraz ewentualnie rozbudowa wykorzystywanych przez Zamawiającego zasobów o dostarczone w ramach niniejszego postępowania dodatkowe komponenty sprzętowe z zachowaniem wykorzystywanych obecnie przez Zamawiającego technologii oraz rozwiązań takich jak wirtualizacja, datastore, kopie zapasowe.
3) instalację Systemu oraz ewentualnych dodatkowych komponentów sprzętowych w trybie wysokiej dostępności tj. w trybie w którym System i komponenty sprzętowe będą pozbawione pojedynczego punktu awarii;
4) dodanie do zaoferowanego Systemu równoważnego źródeł z wszystkich urządzeń wskazanych w tabeli nr 1).
5) konfiguracje i uruchomienie reguł korelacyjnych oraz przeniesienie/odwzorowanie obecnie funkcjonujących w posiadanym systemie SIEM reguł korelacyjnych do Systemu równoważnego
6) przeniesienie wszystkich dotychczas zebranych logów z obecnego systemu SIEM do oferowanego Systemu równoważnego w taki sposób, aby była możliwość ich późniejszego odczytu, przeszukiwania oraz analizy.
7) migrację/wymianę obecnych rozwiązań agentowych służących do przekierowania logów na te wymagane przez System równoważny.
8) przeprowadzenie testów akceptacyjnych wg zaakceptowanych przez Zamawiającego scenariuszy testów. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów.
9) Opracowanie dokumentacji powykonawczej obejmującej w szczególności:
   a) zawierającą dokładny opis architektury wdrożenia, instalacji i konfiguracji zainstalowanych komponentów infrastruktury oraz Systemu
   b) procedury administracyjne,
   c) procedury instalacji i konfiguracji,
   d) procedury bieżących działań administracyjnych,
   e) procedury okresowych/planowanych działań administracyjnych,
   f) procedury aktualizacji Systemu oraz jego poszczególnych komponentów,
   g) procedury włączenia i wyłączenia Systemu oraz sprzętu, na którym jest zainstalowane.
   h) Metody dodawania i usuwania nowych źródeł z Systemu

10) Warsztatowego przekazanie wiedzy dla co najmniej 2 (dwóch) osób, w siedzibie Zamawiającego w Warszawie przy ul. Chmielnej 69 lub w postaci szkolenia on-line, w terminie 2 tygodni od dnia zawarcia umowy obejmujące:
    a) architekturę i konfigurację oprogramowania klasy SIEM,
    b) administrowanie systemem klasy SIEM,
    c) użytkowanie systemu klasy SIEM.

10. Minimalne wymagania dot. ewentualnych dodatkowych komponentów infrastruktury:

Lp.	Cecha	Wymagalne minimalne parametry techniczne
Jeżeli wszystkie opisane poniżej funkcjonalności wymagają dodatkowych licencji i/lub subskrypcji to należy je dostarczyć wraz z urządzeniem lub urządzeniami.		
1	Obudowa	1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 2,5” SAS 12G 2. Dwa dyski twarde SSD skonfigurowane w RAID 1 na potrzeby instalacji hypervisora.
2	Płyta główna	1. Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 2. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
3	Procesor	1. Zainstalowane dwa procesory dedykowane do pracy z zaoferowanym serwerem; umożliwiające spełnienie rekomendowanych wymagań producenta oferowanego Systemu SIEM
4	Pamięć RAM	1. DDR4 lub DDR5 RDIMM 2666 MT/s (lub szybsze) w ilości rekomendowanej przez producenta Systemu równoważnego 2. na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci.
5	Gniazda PCI	1. Minimum 2 x PCIe Gen3 x16 lub nowsze
6	Karty sieciowe	1. sumarycznie przynajmniej 8 portów 10GbE SFP+ dla całego serwera. 2. Wszystkie interfejsy 10GbE muszą umożliwiać bezproblemowe tworzenie zagregowanych połączeń pod kontrolą zainstalowanego systemu operacyjnego serwera
8	Kontroler RAID	1. Sprzętowy kontroler dyskowy 12Gb/s dla dysków SAS i SSD, posiadający min. 4GB nieulotnej pamięci cache

		2. możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60
10	Porty	1. Co najmniej 1 x USB 2.0, 2. Co najmniej 2 x USB 3.0, 3. Co najmniej 2 x VGA (po jednym z przodu i z tyłu) lub inny równoważny tj. HDMI, DisplayPort, DVI
11	Video	1. Zintegrowana karta graficzna
12	Wentylatory	1. Redundantne, 2. Wymiana modułu wentylatora musi być możliwa bezprzerwowo.
13	Zasilacze	1. Redundantne, 2. Hot-Plug
14	Bezpieczeństwo	1. Moduł TPM 2.0 lub nowszy
15	Zarządzanie	Niezależna od zainstalowanego na serwerze systemu operacyjnego karta zarządzania posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) 3. szyfrowane połączenie (min. TLS1.2) oraz autentykacje i autoryzację użytkownika 4. możliwość podmontowania zdalnych wirtualnych napędów 5. wirtualną konsolę z dostępem do myszy, klawiatury 6. wsparcie dla IPv6 7. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer 10. integracja z Active Directory 11. możliwość obsługi przez dwóch administratorów jednocześnie 12. wsparcie dla dynamic DNS 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
16	Zgodność	1. Serwer wraz z komponentami musi się znajdować na HCL VMWare dla ESXI 7.0 U1 oraz ESXI 7.0
17	Wyposażenie	1. Dołączone kompletne okablowanie (dla każdego portu w

	dodatkowe	urządzeniu) SFP+ to SFP+ 10GbE do łączenia bezpośredniego oraz niezbędne moduły SFP+ kompatybilne z urządzeniem i przełącznikami; Zamawiający dopuszcza kompatybilne z serwerami i przełącznikami okablowanie DAC. 2. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
18	Wymagania w zakresie instalacji i konfiguracji	1. Montaż serwera w szafie rack w pomieszczeniu udostępnionym przez Zamawiającego. 2. Podłączenie serwera do listew zasilających PDU. 3. Aktualizacja oprogramowania układowego wszystkich komponentów. 4. Podłączenie do sieci LAN i konfiguracja interfejsów urządzenia w trybie HA 5. Konfiguracja RAID i woluminów serwera. 6. Konfiguracja systemu zdalnego zarządzania.
19	Gwarancja, serwis i wsparcie techniczne producenta	1. 3 letnia gwarancja i serwis realizowany w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany i zabezpieczony kanał komunikacji elektronicznej. 2. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.) oraz system zgłoszeniowy producenta. 3. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej infrastruktury oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 4. Gwarancja i serwis realizowany w trybie 8x5 NBD Onsite Response Time. 5. Zakres wsparcia technicznego 1) Dostęp do pomocy technicznej;

		2) Dostęp do poprawek i nowych wersji oprogramowania i/lub systemu; 3) Dostęp do dokumentacji technicznej; 4) Dostęp do konta wsparcia urządzenia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.
20	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
21	Inne	Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji) Wszystkie oferowane urządzenia muszą być nowe, wyprodukowane nie wcześniej niż w 2022 roku.

F. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważonego:

1. Wykonawca wraz z ofertą wykaże, że oferowane rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, w szczególności przedstawiając Zamawiającemu stosowną dokumentację oprogramowania, potwierdzającą spełnienie przez oferowane oprogramowanie wymagań funkcjonalnych i pozafunkcjonalnych tożsamych jak w oprogramowaniu wskazanym przez Zamawiającego, postanowienia licencji rozwiązania równoważnego jak postanowienia właściwe dla oprogramowania wskazanego przez Zamawiającego oraz warunki świadczonej przez producenta asysty technicznej i konserwacji tożsame z warunkami świadczenia dla oprogramowania wskazanego przez Zamawiającego.
2. Wykonawca zobowiązany jest wykazać, że oferowane przez niego rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, załączając do oferty dowody potwierdzające, że rozwiązanie równoważne spełnia wszystkie parametry równoważności. Dowody powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne poszczególnych parametrów równoważności.
3. Wykonawca na żądanie przygotuje środowisko testowe i scenariusze testowe w celach udowodnienia przez Wykonawcę spełnienia warunków równoważności. Koszty związane z przeprowadzenia jakichkolwiek prac związanych z wykonywaniem testów i przygotowaniem środowiska testowego w tym instalacji, konfiguracji i integracji dostarczonego produktu z systemami Zamawiającego, przy uwzględnieniu m.in. licencji, konsultacji specjalistów, przygotowania scenariuszy testowych, szkoleń ponosi w całości Wykonawca.

4. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 5 minut.
5. Zaoferowane rozwiązanie równoważne musi być w pełni kompatybilne z istniejącymi rozwiązaniami w środowisku.
6. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W przypadku zaoferowania rozwiązań równoważnych Zamawiający wymaga od Wykonawcy przedstawienia dokumentów potwierdzających, czy i w jakim zakresie w jego opinii zachodzi równoważność rozwiązań/ produktów i w zakresie jakich elementów (parametrów, funkcji lub cech określonych przez Zamawiającego) określonych w OPZ.