SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa wraz z przedłużeniem licencji dla posiadanego systemu SIEM opartego na architekturze Splunk Enterprise wraz z usługą serwisu i wsparcia technicznego, z okresem obowiązywania od dnia 07.06.2022 r.

1. Przedmiot zamówienia obejmuje:

1.1 Sprzedaż i dostawę licencji dla posiadanego przez Zamawiającego oprogramowania klasy „SIEM" z okresem obowiązywania od dnia 07.06.2022 oraz wsparcia producenta przez 18 miesięcy, liczonym od dnia uruchomienia licencji, w modelu tradycyjnym na istniejącej infrastrukturze Zamawiającego.

1.2 Przeprowadzenie przez Wykonawcę warsztatowego przekazania wiedzy dla co najmniej 2 (dwóch) osób, którego zakres obejmuje;

a. Architekturę i konfigurację oprogramowania klasy SIEM,
b. Administrowanie systemem klasy SIEM,
c. Użytkowanie systemu klasy SIEM.

1.3 Świadczenie serwisu i wsparcia technicznego Wykonawcy dla oprogramowania przez okres 18 miesięcy liczony od dnia uruchomienia licencji, tj. od 07.06.2022 r.

2. Wymagania dotyczące dostawy oprogramowania oraz licencji:

2.1 Dostawa musi zostać zrealizowana w terminie do 10 dni roboczych od dnia podpisania Umowy.

2.2 Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca.

2.3 Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski.

2.4 Dostawa, instalacja, konfiguracja oprogramowania, aplikacji, modułów wymaganych do zbudowania zaoferowanego Systemu, musi być zgodna z wymaganymi funkcjonalnościami oraz oczekiwaniami Zamawiającego.

2.5 Dostawa, instalacja, licencji wymaganych do poprawnej pracy Systemu, musi być zgodna z wymaganymi funkcjonalnościami, przy minimalnym zapewnieniu wielkości gromadzonych logów/danych na poziomie 60 GB dziennie.

2.6 Zamówione licencje muszą być dostarczone do Zamawiającego w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie plików

wygenerowanych i przesłanych przez Wykonawcę na wskazany przez Zamawiającego adres e-mail.

3. Wymagania dot. zakresu usług

3.1 Warsztatowe przekazanie wiedzy zgodnie ze specyfikacją Zamawiającego.

3.2 Świadczenie serwisu i wsparcia technicznego Wykonawcy, przez okres 18 miesięcy, liczony od dnia uruchomienia licencji, tj. od 07.06.2022 r.

3.3 Usługa wsparcia technicznego producenta świadczona przez okres 18 miesięcy, liczony od dnia uruchomienia licencji, tj. od 07.06.2022 r.

`

4. Wymagana funkcjonalność systemu

4.1 System nie może posiadać ograniczeń w postaci ilości urządzeń, z których pobierane są logi, jak również liczby źródeł generowanych logów.

4.2 System musi zapewniać wydajność parsowania logów, których wielkość dochodzi do 60 GB oraz dla których częstość zdarzeń na sekundę (EPS) może dochodzić do 36000 EPS.

4.3 Zaoferowany 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).

4.4 System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę na co najmniej 12TB danych.

4.5 System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych

4.6 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.

4.7 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.

4.8 System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne.

4.9 System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności, związanych z analizą danych obejmującą:

a. mechanizmy pobierania danych,
b. raporty, dashboardy i formularze,
c. nowe funkcje analityczne,
d. nowe sposoby wizualizacji,
e. mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent.

Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta.

4.10 Musi istnieć możliwość tworzenie 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).

4.11 System musi umożliwiać integrację danych gromadzonych z różnych źródeł: aplikacji, baz użytkowników, w tym katalogu Active Directory. Dane powinny być dostępne jako spójna informacja na poziomie interfejsu analitycznego systemu.

4.12 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.

4.13 Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi, takich klient SSH lub RDP.

4.14 System powinien 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

4.15 System musi umożliwiać pobieranie logów z co najmniej następującymi protokołami:

a. syslog UDP/TCP,

b. trap SNMP,
c. 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),
d. pliki tekstowe,
e. WMI,
f. NetFlow v5 i v9, sFlow, jFlow, IPFIX.

Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

4.16 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.

4.17 System musi posiadać interfejs programowania aplikacji (API) w postaci bibliotek programistycznych dla języków: Java, Python, JavaScript, PHP, Ruby oraz C#.

4.18 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:
a. DHCP,
b. DNS,
c. HTTP,
d. IMAP,
e. SIP,
f. SMB,
g. SMTP.

Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.

4.19 System musi posiadać udokumentowany interfejs REST (Representational State Transfer) umożliwiający integrację z zewnętrznymi systemami teleinformatycznymi.

4.20 Mechanizm przechowywania logów/danych/zdarzeń wdrożonego rozwiązania musi uniemożliwiać nieupoważnione usunięcie całości lub części logów, danych, raportów i innych informacji oraz zapewniać dostęp do nich tylko dla uprawnionych, uwierzytelnionych użytkowników.

4.21 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.

4.22 Zaoferowany 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).

4.23 Licencja Systemu nie może ograniczać liczby elementów gromadzących oraz analizujących logi.

4.24 Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http_user_agent) oraz opcjonalnie agregacji danych.

4.25 System musi zapewnić nieprzerwaną kontynuację pracy w przypadku awarii jednego z centrum przetwarzania danych lub dowolnego elementu infrastruktury tego Systemu.

4.26 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.

4.27 Tabele i wykresy prezentowane na bazie dostarczonych logów/danych muszą posiadać funkcję drill-down, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie interfejs powinien pokazywać odpowiadające im logi/dane.

4.28 Musi istnieć możliwość definiowania akcji typu drill down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny 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.

4.29 Rozwiązanie musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do Rozwiązania.

4.30 System musi automatycznie (tj. bez uprzedniego definiowania schematu danych wejściowych) analizować dane zdarzanie (dzienniki systemowe w formie Syslog, Netflow, itp.) pod kątem zawartości i struktury danych. Wynikiem analizy powinny

być informacje mapowane w formacie łatwym do późniejszego wyszukiwania i analizy, np. w strukturach klucz-wartość.

4.31 Rozwiązanie powinno 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

4.32 Rozwiązanie 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.

4.33 Mechanizm pobierania logów/danych ze źródeł, powinien 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.

4.34 Rozwiązanie 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.

4.35 System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.).

4.36 System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą XML. System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON.

4.37 System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach.

4.38 System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość, np. „user=jkowalski” powinno tworzyć pole „user” o wartości „jkowalski”.

4.39 System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.

4.40 Zaoferowany System musi umożliwiać wydajną pracę użytkownika przeglądającego zdarzenia i generującego raporty oraz samego Systemu, w szczególność parsowania danych których wielkość dochodzi do 60 GB dziennie.

4.41 Zaoferowany System musi umożliwiać parsowanie logów o długości co najmniej 10000 znaków oraz zawierających więcej niż jedna linię.

4.42 Zaoferowany System musi umożliwiać tworzenie bazy definicji formatów logów.

4.43 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.).

4.44 System musi automatycznie proponować definicje pól, dla poszczególnego typu logów wykorzystywanych do dalszej analizy oraz tworzyć statystyki występowania poszczególnych wartości tych pól.

4.45 System musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych.

4.46 System musi umożliwiać definiowanie pól za pomocą wyrażeń regularnych (REGEX).

4.47 System musi umożliwiać w czasie rzeczywistym wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX).

4.48 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).

4.49 System musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną.

4.50 System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł.

4.51 System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danej Systemu.

4.52 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.

4.53 Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.

4.54 Rozwiązanie 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).

4.55 W zaoferowanym 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.

4.56 System musi wspierać pracę użytkowników o różnych rolach i w następujących obszarach:

a. Analiza zdarzeń w obszarze bezpieczeństwa teleinformatycznego,
b. Analiza pracy systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń teleinformatycznych,
c. Analiza pracy aplikacji wdrażanych/tworzonych przez pracowników NCBR.

4.57 System musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych.

4.58 Rozwiązanie musi umożliwiać jednoczesną pracę analityczną co najmniej dla 20-u użytkowników.

4.59 Licencja Rozwiązania musi umożliwiać utworzenie kont i pracę dla co najmniej 20-u użytkowników.

4.60 System musi umożliwiać odseparowanie środowiska pracy użytkowników o różnych rolach.

4.61 Wdrożony System musi być odporny na ataki sieciowe.

4.62 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.

4.63 System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:

a. Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych,
b. Możliwość przypisania incydentu do osoby,
c. Możliwość zmiany statusu i priorytetu incydentu,
d. Możliwość tworzenia komentarzy,

e. Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy.
f. Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki.
g. Możliwość raportowania wydajności obsługi incydentów.

4.64 Możliwość zintegrowania z systemami monitoringu np. Zabbix, Solarwinds, w celu monitorowania liczników wydajnościowych oraz dostępności serwisów w kontekście użytkownika/systemu końcowego.

5. Wymagania odnośnie warsztatowego przekazania wiedzy:

5.1 Zamawiający wymaga przeprowadzenie przez Wykonawcę autorskiego warsztatowego przekazania wiedzy, o którym mowa w pkt 1.4 dla co najmniej 2 (dwóch) osób, w siedzibie Zamawiającego w Warszawie przy ul. Nowogrodzkiej 47a lub w postaci szkolenia on-line, w terminie obowiązywania umowy.

6. Zakres wsparcia technicznego i serwisu Rozwiązania

6.1. Zakres wsparcia producenta oprogramowania klasy SIEM:

6.1.1. Dostęp do pomocy technicznej oprogramowania;
6.1.2. Dostęp do poprawek i nowych wersji Systemu;
6.1.3. Dostęp do dokumentacji technicznej;
6.1.4. Dostęp do konta wsparcia oprogramowania SIEM, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta oprogramowania.

6.2. Zakres serwisu i wsparcia technicznego dostawcy Systemu:

6.2.1. 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:

- System zgłoszeń musi obejmować następujące kanały zgłoszeń: serwis WWW, poczta elektroniczna, telefon.
- W ramach systemu zgłoszeń zapewnienie kanału WWW do śledzenia i aktualizacji zarejestrowanych zgłoszeń oraz zapewnienie możliwości automatycznego dodawania wpisów w systemie poprzez e-mail.

6.2.2. Usuwanie usterek i błędów z zachowaniem poniższych zasad:

- Jako błąd krytyczny uznana zostanie sytuacja z powodu której System nie funkcjonuje lub kiedy nie można wykonać w nim kluczowych czynności.

- 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.
- 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).
- 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 10 dni roboczych od przyjęcia zgłoszenia.
- Usunięcie innych błędów nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- Usunięcie usterek nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- 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.
- Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni od daty jego wdrożenia.

6.2.3. Utrzymanie i aktualizacje zaimplementowanych dashboardów, raportów i alertów stworzonych na potrzeby Zamawiającego.

6.2.4. Świadczenie usług konsultacyjnych w zakresie funkcjonowania Systemu SIEM:

- Wymiar: do 72 roboczogodzin;

- Dostępność: dni robocze od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy;
- Miejsce: zdalnie;
- Realizacja zadań wynikających z zakresu umowy;
- Wsparcie w pracach rozwojowych i zadaniach administracyjnych.

6.2.5. Wykonawca zapewni wsparcie techniczne przez okres 24 lub 30 miesięcy, liczony od dnia uruchomienia licencji, tj. 07.06.2022 r. Objęcie usługami wsparcia technicznego i serwisu Systemu SIEM musi zapewnić Zamawiającemu pełną gotowość Wykonawcy do świadczenia opisanych w niniejszej specyfikacji usług od pierwszego dnia obowiązywania licencji. Ponadto, świadczone usługi nie mogą negatywnie wpływać na zintegrowane z Systemem SIEM aplikacje biznesowe i inne systemy bezpieczeństwa informacji.

6.2.6. 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 Rozwiązania.

7. Opis posiadanych przez Zamawiającego licencji, wsparcia dla posiadanego Systemu SIEM oraz infrastruktury:

7.1. Licencja Splunk Enterprise 50GB/day, ze wsparciem producenta ważna do dnia 2022-06-06.

7.2. Licencja Splunk Enterprise Security 50GB/day, ze wsparciem producenta ważna do dnia 2022-06-06.

7.3. Zamawiający posiada uruchomione następujące maszyny wirtualne dla w/w rozwiązania:

a. Splunk MC,
b. Splunk DS Lic Srv,
c. Splunk HFW,
d. Splunk - Indexer 1,
e. Splunk - Indexer 2,
f. Splunk – SH.