**SPECYFIKACJA OFEROWANEGO PRODUKTU**

# **System klasy SIEM\*:**

Producent: ……………………………………………………………………………………………………………………………………………

Nazwa oprogramowania: …………………………………………………………………………………………………………………………..

Typ licencji: …………………………………………………………………………………………………………………………………………..

\*Jeżeli system klasy SIEM wymaga większej liczby licencji / subskrypcji lub wsparcia producenta niż określono, Wykonawca umieszcza stosowne informacje.

\*\* W przypadku zaoferowania rozwiązania równoważnego Oferent wypełnia pkt: 1.,2.,3.,6.,7.,8. w przypadku zaoferowania oferty na rozbudowę systemu posiadanego przez Zamawiającego, Oferent wypełnia pkt. 1.,2.,3.,4.,5.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LP\*\*** | **Wymagania** | **Minimalne** | **Opcjonalne****(dodatkowo punktowane w kryteriach oceny ofert)** | **Parametry/rozwiązania oferowane przez Wykonawcę lub informacja o spełnieniu wymagań minimalnych** |
| **1.** | **Wymagania ogólne dla systemu SIEM** |
| 1.1 | Oferowane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja musi pochodzić od producenta i być świadczona przez sieć serwisową producenta, również na terenie Polski. | TAK |  |  |
| 1.2 | Wdrażany system musi zostać objęty serwisem oraz wsparciem technicznym producenta wdrażanego rozwiązania przez okres obowiązywania licencji od dnia jej uruchomienia oraz serwisem i wsparciem technicznym Wykonawcy przez okres obowiązywania Umowy zgodnie z warunkami Zamówienia. | TAK |  |  |
| **2.** | **Wymagania dla architektury systemu klasy SIEM** |
| 2.1 | Komponenty systemu SIEM mogą być zainstalowane w infrastrukturze PGL LP (środowisko wirtualne VMware ESXi 7.0 lub nowsze) oraz zagwarantuje co najmniej trzy wydzielone serwery każdy o parametrach CPU 32core / vCPU 64core 2,9GHz oraz sumaryczną pamięć nie większą niż 352GB RAM oraz dyski SSD obsługujące min. 800 IOPS o pojemności 15TB na retencję danych Hot, Warm przez okres 7 dni, Cold 30 dni oraz Archived (Frozen) z wykluczeniem dysków SSD na okres 3 miesięcy. W przypadku gdy oferowane rozwiązanie wymaga większej ilości zasobów sprzętowych niż określa Zamawiający, Wykonawca dostarczy odpowiednią platformę sprzętowo-programową w oparciu o środowisko wirtualnie VMware ESXi 7.0 lub nowsze wraz z odpowiednimi licencjami | TAK |  |  |
| **3.** | **Wymagania dla licencji oraz systemu gwarancyjnego rozwiązania posiadanego „Splunk Enterprise” lub systemu równoważnego** |
| 3.1 | W wyniku rozbudowy będącej przedmiotem postępowania, Zamawiający oczekuje iż będzie posiadał licencje oprogramowania oraz pakiety usług wsparcia producenta „Splunk Enterprise - Term License with Standard Success Plan - GB/day” o wolumenie danych nie mniejszym niż 250 GB/dzień oraz okresem obowiązywania 24 miesięcy. | TAK | TAK | *Informacja umieszczona w formularzu oferty* |
| 3.2 | Dostawa, licencji dla posiadanego przez Zamawiającego oprogramowania musi obowiązywać od dnia 29.12.2022r. oraz zapewniać wsparcie producenta przez okres minimum 24 miesięcy kalendarzowych, liczonych od dnia uruchomienia licencji w infrastrukturze Zamawiającego. | TAK |  |  |
| 3.3 | Wykonawca wraz z dostawą licencji przekaże warunki gwarancji i procedury awarii, dostępne kanały komunikacyjne z serwisem Producenta i Wykonawcy. | TAK |  |  |
| 3.4 | Wsparcie wykonawcy oraz serwis wdrożonego systemu zgodnie z okresem obowiązywania Umowy. | TAK |  |  |
| 3.5 | Wykonawca w ramach wsparcia zapewni Zamawiającemu 24 godziny konsultacji w formie telefonicznej lub na wskazany przez Wykonawcę adres e-mail w skali miesiąca przez cały okres obowiązywania Umowy. | TAK |  |  |
| 3.6 | Przyjmowanie w ramach serwisu zgłoszeń Zamawiającego przez 24 godziny na dobę, 7 dni w tygodniu. | TAK |  |  |
| 3.7 | Czas naprawy nie może przekroczyć dwudziestu czterech godzin liczonych od chwili wysłania zgłoszenia w dni robocze, zgłoszenia wysłane w ostatni dzień tygodnia roboczego zrealizowane będą w najbliższy dzień roboczy do godz.: 15:00. Czas naprawy rozumiany jest jako czas usunięcia przez Wykonawcę zgłoszonego przez Zamawiającego problemu liczonego od chwili przekazania informacji Wykonawcy w formie elektronicznej lub telefonicznej na wskazane przez Wykonawcę źródła kontaktu. | TAK |  |  |
| 3.8 | Możliwość aktualizacji oprogramowania w tym poprawek bezpieczeństwa przez dostęp do zasobów producenta. | TAK |  |  |
| 3.9 | Bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail, w języku Polskim oraz serwis WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją systemu w trybie całodobowym w każdy dzień tygodnia 24/7/365. | TAK |  |  |
| 3.10 | Możliwość pobrania bezpośrednio od producenta nowych wydań oprogramowania, w ramach ogólnie dostępnej oferty producenta. | TAK |  |  |
| 3.11 | W okresie obowiązywania gwarancji, Wykonawca będzie świadczył usługi wsparcia przez wykwalifikowanych pracowników, posiadających ugruntowaną wiedzę potwierdzoną certyfikatami w zakresie systemu będącego przedmiotem Umowy. | TAK |  |  |
| 3.12 | Jeżeli wykorzystanie którejkolwiek z wymienionych w OPZ funkcjonalności wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć | TAK |  |  |
| **4.** | **Wymagania dla rozbudowy rozwiązania posiadanego „Splunk Enterprise”** |
| 4.1 | Wykonawca dostarczy niezbędne pakiety wsparcia producenta na całość rozwiązania ważne przez cały okres obowiązywania Licencji | TAK |  |  |
| 4.2 | Rekonfiguracja aktualnie działającego środowiska w tym dostosowanie platformy do zbierania zdarzeń ze źródeł Zamawiającego: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint, EMM, NSX, VMware, Serwery Pocztowe, Serwery Spam-u, urządzenia sieciowe Cisco, Cisco ISE, Ubiquity, syslog-ng, logi systemowe Windows Server, logi systemowe Linux, logi web serwisów (głównie Apache/Tomcat), Radius, Active Identity, Własne dedykowane rozwiązania systemowe. | TAK |  |  |
| 4.3 | Architektura systemu musi być tak dostosowana aby zapewnić optymalną wydajność i skalowalność uwzględniając min. 1 serwer służący do przeszukiwania zbiorów oraz 2 serwery odpowiedzialne za indeksowanie danych. Zamawiający szacuje iż 80% ruchu zdarzeń będzie generowanie z 5 systemów tj. Firewall Centralny, Active Directory, oraz urządzenia brzegowe klasy UTM oddziałów terenowych zamawiającego w ilości ~ 500 szt. scentralizowane do jednego repozytorium w węźle centralnym wraz z ochroną Endpoint. | TAK |  |  |
| 4.4 | Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy przez cały okres obowiązywania Umowy dla rozbudowanego rozwiązania. | TAK |  |  |
| **5.** | ***Warunki dla warsztatowego przekazania wiedzy wraz ze szkoleniem dla rozbudowy systemu „Splunk Enterprise”*** |
| 5.1 | Wykonawca przeprowadzi szkolenie powdrożeniowe | TAK |  |  |
| 5.2 | Liczba uczestników – do 8 osób | TAK |  |  |
| 5.3 | Program szkolenia musi zawierać całość zagadnień obejmujących, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie. | TAK |  |  |
| 5.4 | Szkolenie zostanie przeprowadzone w lokalizacji Zamawiającego w miejscu wdrożenia rozwiązania lub w formie Zdalnej na środowisku produkcyjnym oraz na środowisku szkoleniowym przygotowanym przez Wykonawcę w celu omówienia elementów wrażliwych mogących doprowadzić do uszkodzenia środowiska produkcyjnego Zamawiającego. | TAK |  |  |
| 5.5 | Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF. | TAK |  |  |
| 5.6 | Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim. | TAK |  |  |
| 5.7 | Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie. | TAK |  |  |
| 5.8 | Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem. | TAK |  |  |
| 5.9 | Wszyscy uczestnicy szkolenia otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia. | TAK |  |  |
| 5.10 | Szkolenie przeprowadzone nienależycie Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia szkolenia podlegających powtórzeniu | TAK |  |  |
| **6.** | **Wymagania dla rozwiązania równoważnego systemu klasy SIEM** |
| 6.1 | Rozwiązanie musi pochodzić z oferty jednego producenta i być systemem komercyjnym, z zastrzeżeniem iż nie może to być rozwiązanie typu „open source”. | TAK |  |  |
| 6.2 | Rozwiązanie klasy SIEM musi znajdować się w kwadracie „Leaders” raportu Gartnera „Magic Quadrant for Security Information and Event Management June 2022r.” | TAK |  |  |
| 6.3 | System SIEM musi istnieć na rynku co najmniej 5 lat oraz posiadać wsparcie techniczne producenta w języku polskim | TAK |  |  |
| 6.4 | Oferowane rozwiązanie musi umożliwić wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie: monitorowania usług, wydajności aplikacji. Rozwiązanie powinno posiadać udokumentowane wdrożenia o podobnej skali. | TAK |  |  |
| 6.5 | W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego, Wykonawca dokona migracji danych z obecnie używanego rozwiązania SIEM „Splunk Enterprise” oraz dostosuje strukturę oprogramowania równoważnego do działającego systemu oraz zastosowanych w nim rozwiązań w infrastrukturze Zamawiającego. | TAK |  |  |
| 6.6 | W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie działać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego. | TAK |  |  |
| 6.7 | Oprogramowanie równoważne nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania. | TAK |  |  |
| 6.8 | Zaoferowane rozwiązanie musi umożliwiać Zamawiającemu skalowalność , rozbudowę architektury w przypadku wzrostu wymagań wydajnościowych i pojemnościowych wynikających z przekazywania, gromadzenia oraz zwiększania poziomu szczegółowości logowanych zdarzeń (logów / danych). | TAK |  |  |
| 6.9 | Musi istnieć możliwość rozbudowy środowiska o dodatkowe węzły poprawiające wydajność systemu bez konieczności zakupu dodatkowych licencji lub modułów. | TAK |  |  |
| 6.10 | Zaoferowany System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej w celu przechowywania danych archiwalnych. | TAK |  |  |
| 6.11 | Rozwiązanie musi posiadać możliwość planowanego przenoszenia danych na podstawie czasu lub okresu na pamięci masowe niższego poziomu. | TAK |  |  |
| 6.12 | Rozwiązanie nie może powodować utraty danych w przypadku przekroczenia limitu dziennego pobierania logów w odniesieniu do wykorzystywanej licencji w danym momencie. | TAK |  |  |
| 6.13 | System musi umożliwiać integrację danych gromadzonych z różnych źródeł, przetwarzane dane powinny być dostępne jako spójna informacja na poziomie analizy zdarzeń. | TAK |  |  |
| 6.14 | Zaoferowany system musi posiadać mechanizm uniemożliwiający usuwanie całości lub części logów, danych przez nieuprawnionych użytkowników. Dostęp do danych musi być dostępny tylko dla uprawnionych, uwierzytelnionych użytkowników. | TAK |  |  |
| 6.15 | Rozwiązanie musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych. | TAK |  |  |
| 6.16 | Tabele i wykresy prezentowane na bazie dostarczonych logów / danych muszą posiadać funkcję drążenia w dół, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie, interfejs powinien pokazywać odpowiadające im logi / dane. | TAK |  |  |
| 6.17 | Rozwiązanie powinno pozwalać na analizę standardowych logów infrastrukturalnych generowanych przez systemy operacyjne, firewalle, urządzenia sieciowe (przełączniki, routery, loadbalancery, itd.) systemy bezpieczeństwa IPS/IDS/ Application & URL Filtering / Anti-Bot, WAF itd. | TAK |  |  |
| 6.18 | Rozwiązanie powinno pozwalać na analizę niestandardowych logów wygenerowanych przez aplikacje własne. | TAK |  |  |
| 6.19 | System musi posiadać możliwość przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej z następujących źródeł: Cisco ASA, F5 , A10, CISCO (przełączniki, routery, firewalle), systemu operacyjne (Red Hat, Microsoft Windows), usługi serwerowe (DNS, DHCP, WWW (Apache, IIS)), Oracle, SQL Server, Vmware vSphere, Logi Windows Events (Logi Application, Security, System I inne) , logi z ruchu sieciowego poprzez Netflow. | TAK |  |  |
| 6.20 | Zaoferowane rozwiązanie 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 przez zaoferowane rozwiązania zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC, | TAK |  |  |
| 6.21 | Rozwiązanie musi umożliwiać następujące funkcje dotyczące pracy nad logami: - Rozwiązanie musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię, - Rozwiązanie musi umożliwiać tworzenie bazy definicji formatów logów, - Rozwiązanie musi wyszukiwać́ czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać́ go do reguł korelacyjnych, - Rozwiązanie musi umożliwiać́ wyszukiwanie zdarzeń́ w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX) lub gotowych wzorców wyboru np: adres IP źródłowy/docelowy, port, protokół, - Rozwiązanie musi umożliwiać́ tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną, - System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł, oraz korelować dane w czasie rzeczywistym, - Reguły korelacji powinny być tworzone i zarządzane w interfejsie systemu, bez potrzeby użycia dodatkowych narzędzi firm trzecich, - Rozwiązanie musi umożliwiać́ wykrywanie sytuacji niestandardowej 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), - Zaoferowane rozwiązanie musi umożliwiać́ łatwe i samodzielne tworzenie reguł parsowania logów/danych, tworzenie widoków/raportów kolejnych/nowych dowolnych źródeł danych, przez pracowników Zamawiającego po przeprowadzonych szkoleniach oraz warsztatowe przekazanie wiedzy. | TAK |  |  |
| 6.22 | Rozwiązanie musi posiadać następujące funkcje dotyczące raportowania: 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 | TAK |  |  |
| 6.23 | Rozwiązanie musi zapewnić́ rozliczność́ działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych | TAK |  |  |
| 6.24 | Rozwiązanie musi umożliwiać́ odseparowanie środowiska pracy użytkowników o rożnych rolach. | TAK |  |  |
| 6.25 | Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zawarte w zewnętrznych repozytoriach: Katalogi LDAP, Bazy danych, Dane geolokalizacyjne. | TAK |  |  |
| 6.26 | System musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach). | TAK |  |  |
| 6.27 | Rozwiązanie musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych | TAK |  |  |
| 6.28 | System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI jak i języka zapytań charakterystycznego dla danego systemu SIEM. | TAK |  |  |
| 6.29 | Musi istnieć możliwość zastosowania reguł korelacyjnych dla danych historycznych w celu wykrycia podobnych zdarzeń w przeszłości. | TAK |  |  |
| 6.30 | System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania. Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie. | TAK |  |  |
| 6.31 | Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.). | TAK |  |  |
| 6.32 | 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. | TAK |  |  |
| 6.33 | Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto. | TAK |  |  |
| 6.34 | System musi umożliwiać prezentację zdarzeń związanych z użytkownikiem niezależnie od tego z jakiego konta korzystał. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane. | TAK |  |  |
| 6.35 | System musi umożliwiać korzystanie z zewnętrznych wskaźników kompromitacji (ang. IOC). | TAK |  |  |
| **7.** | **Wymagania dla wdrożenia rozwiązania równoważnego** |
| 7.1 | Wykonawca dostarczy niezbędne licencje i pakiety wsparcia producenta równoważne na całość rozwiązania ważne przez cały okres obowiązywania Licencji | TAK |  |  |
| 7.2 | Migracja danych i ustawień aktualnie działającego systemu klasy SIEM oraz dostosowanie platformy do zbierania zdarzeń ze wskazanych źródeł | TAK |  |  |
| 7.3 | Zapewnienie logowania danych ze źródeł: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint, EMM, NSX, VMware, Serwery Pocztowe, Serwery Spam-u, urządzenia sieciowe Cisco, Cisco ISE, Ubiquity, syslog-ng, logi systemowe Windows Server, logi systemowe Linux, logi web serwisów (głównie Apache/Tomcat), Radius, Active Identity, Własne dedykowane rozwiązania systemowe | TAK |  |  |
| 7.4 | Architektura systemu musi być tak dostosowana aby zapewnić optymalną wydajność i skalowalność uwzględniając min. 1 serwer służący do przeszukiwania zbiorów oraz 2 serwery odpowiedzialne za indeksowanie danych. Zamawiający szacuje iż 80% ruchu zdarzeń będzie generowanie z 5 systemów tj. Firewall Centralny, Active Directory, oraz urządzenia brzegowe klasy UTM oddziałów terenowych zamawiającego w ilości ~ 500 szt. scentralizowane do jednego repozytorium w węźle centralnym wraz z ochroną Endpoint | TAK |  |  |
| 7.5 | Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy przez cały okres obowiązywania Umowy dla rozbudowanego rozwiązania | TAK |  |  |
| **8.** | ***Warunki dla warsztatowego przekazania wiedzy wraz ze szkoleniem dla rozwiązania równoważnego*** |
| 8.1 | Wykonawca przeprowadzi szkolenie obejmujące zakresem, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu u Zamawiającego oraz Szkolenie Certyfikowane przez autoryzowany ośrodek szkoleniowy dla oferowanego rozwiązania równoważnego | TAK |  |  |
| 8.2 | Liczba uczestników szkolenia powdrożeniowego oraz szkolenia certyfikowanego – do 8 osób | TAK |  |  |
| 8.3 | Program szkolenia musi zawierać całość zagadnień obejmujących, podstawową administrację, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie. | TAK |  |  |
| 8.4 | Szkolenie powdrożeniowe zostanie przeprowadzone w lokalizacji Zamawiającego w miejscu wdrożenia rozwiązania lub w formie Zdalnej na środowisku produkcyjnym oraz na środowisku szkoleniowym przygotowanym przez Wykonawcę w celu omówienia elementów wrażliwych mogących doprowadzić do uszkodzenia środowiska produkcyjnego Zamawiającego | TAK |  |  |
| 8.5 | Szkolenie certyfikowane dla produktów producenta rozwiązania równoważnego zostanie przeprowadzone przez autoryzowany ośrodek szkoleniowy w formule Zdalnej lub w autoryzowanym ośrodku szkoleniowym na terenie Polski. | TAK |  |  |
| 8.6 | Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF | TAK |  |  |
| 8.7 | Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim | TAK |  |  |
| 8.8 | Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie. | TAK |  |  |
| 8.9 | Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem | TAK |  |  |
| 8.10 | Szkolenie przeprowadzone nienależycie Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia szkolenia podlegających powtórzeniu. | TAK |  |  |
| 8.11 | Wszyscy uczestnicy szkolenia otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia. | TAK |  |  |