**Szczegółowy opis przedmiotu zamówienia**

Przedmiotem szacowania jest zakup licencji (opartych na subskrypcjach), dostarczenie, uruchomienie i wdrożenie produkcyjne rozwiązania informatycznego, obejmującego funkcjonalność analizy luk bezpieczeństwa i podatności dla środowisk wirtualnych, automatyzacji audytów bezpieczeństwa oraz świadczenie innych usług towarzyszących zgodnie z poniższą specyfikacją:

1. Maksymalna ilość subskrypcji rozwiązania objętych wdrożeniem –
   1. 500 CPU (fizyczne procesory)
   2. 1000 systemów operacyjnych maszyn wirtualnych
   3. 50 Kubernetes
2. Wsparcie techniczne Producenta dla subskrypcji i gwarancja na okres 36 miesięcy od dnia podpisania Protokołu Odbioru Dostawy licencji na oprogramowanie.
3. Usługi towarzyszące Wykonawcy obejmujące:
   1. Usługi Instalacyjno-Wdrożeniowe i warsztaty wdrożeniowe dla administratorów IT,
   2. Usługi wsparcia eksperckiego Wykonawcy do wdrożonego rozwiązania,

opisane poniżej w OPZ.

1. Zamawiający przewiduje możliwość wdrożenia rozwiązania w różnych fizycznych lokalizacjach.
2. Zamawiający nie dopuszcza rozwiązania, którego Moduły i komponenty znajdują się lub będą instalowane w chmurze (ang. cloud) oraz w jakiejkolwiek usłudze kolokacji.

**I Wymagania ogólne**

1. Oferowane rozwiązanie musi posiadać wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source.
2. Oferowane rozwiązanie musi istnieć na rynku co najmniej 3 lat oraz posiadać wsparcie techniczne producenta w języku angielskim lub polskim.
3. Oferowane rozwiązanie musi pochodzić tylko z oficjalnych kanałów dystrybucyjnych Producenta na terenie Unii Europejskiej.
4. Oferowane rozwiązanie musi stanowić jednolite środowisko programowe, być kompletne i pochodzić od tego samego Producenta , tj. wszystkie komponenty technologiczne i licencje wymagane do poprawnego działania muszą współpracować ze sobą bez konieczności stosowania dodatkowych elementów nie będących standardową częścią oferowanego rozwiązania, .
5. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
6. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
7. Wszystkie elementy dostarczanego rozwiązania muszą być w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia.
8. Całość przetwarzania danych zebranych z analizowanego środowiska typu: nazwy hostów ESXi, adresy IP, klucze licencyjne, identyfikatory klientów lub numery kont uprawnień musi odbywać się w infrastrukturze Jednostek.
9. Zamawiający nie dopuszcza instalacji rozwiązania i przetwarzania danych Zamawiającego lub Jednostek w rozwiązaniach chmurowych oraz w jakiejkolwiek usłudze kolokacji .
10. Żaden z elementów rozwiązania na dzień wdrożenia nie może być przeznaczony przez Producenta do wycofania z produkcji lub sprzedaży.
11. Czynności związane z wdrożeniem i konfiguracją rozwiązania w infrastrukturze Jednostek muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Zamawiającego.
12. Wykonawca zobowiązuje się w szczególności:
    * 1. dostarczyć, wdrożyć, uruchomić i skonfigurować rozwiązanie,
      2. wykonać analizę przedwdrożeniową oraz dokumentację projektu technicznego oraz dokumentację powdrożeniową;
      3. uzgodnić z Jednostką harmonogram wdrożenia;
      4. zapewnić subskrypcję na okres 36 miesięcy od dnia podpisania Protokołu Odbioru Dostawy Licencji na oprogramowanie, wymaganych do prawidłowego działania rozwiązania jako całości, jak i poszczególnych jego elementów. Licencjobiorcami oraz podmiotami uprawnionymi do korzystania z rozwiązania są wszystkie Jednostki czyli Sądy Powszechne oraz Ministerstwo Sprawiedliwości.
      5. przenieść na Jednostki autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.
      6. udzielić Gwarancji na wykonane wdrożenie w ramach Umowy od daty podpisania Protokołu Odbioru Wdrożenia na okres trwania subskrypcji licencji oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wykonanych usług wdrożeniowych dostarczonego rozwiązania w ramach wynagrodzenia wynikającego z Umowy.
13. Wykryte zagrożenia muszą być prezentowane w formie kompleksowego opisu wraz ze sposobem ich rozwiązania. Jeżeli zagrożenie dotyczy wielu elementów, musi istnieć możliwość ich wyszukiwania listy tych obiektów. Rozwiązanie musi dostarczać spójny, jednorodny interfejs graficzny, umożliwiający wykonanie wszystkich czynności. – przeglądanie wyników analizy bezpieczeństwa środowiska czy konfigurację systemu.
14. Rozwiązanie musi wykonywać wszystkie analizy w środowisku Jednostki bez konieczności komunikacji z Internetem. Zebrane dane oraz wyniki analiz przechowywane są w wewnętrznej bazie danych rozwiązania i zebrane dane nie będą przesyłane poza środowisko Jednostki.
15. Rozwiązanie może korzystać z sieci Internetowej tylko do celu automatycznego pobierania aktualizacji systemu lub biblioteki zagrożeń i podatności ze zdefiniowanych źródeł tj. stron www producenta tego rozwiązania.
16. Rozwiązanie musi umożliwiać aktualizowanie rozwiązania, nowych wersji bibliotek zagrożeń i podatności, itp. w trybie „offline” tj. bez dostępu do Internetu i „online” tj. z dostępem do Internetu. Sposób realizacji aktualizacji zależeć musi od ustawiań konfiguracyjnych i może być zmieniany w dowolnym momencie przez Jednostkę.
17. Rozwiązanie musi mieć możliwość filtrowanie zebranych wyników i ich exportu do pliku csv lub pdf.
18. Rozwiązanie powinno dostarczać gotowe rozwiązanie dla zagrożeń w formie dedykowanego i gotowego do użycia skryptu PowerCLI lub Ansible.
19. Rozwiązanie musi być dostarczone w formie przygotowanego przez producenta gotowych obrazów maszyn wirtualnych VMware vApp.
20. Rozwiązanie musi analizować i wykrywać znane podatności w środowiskach vSphere, vSAN, NSX-V, NSX-T, Horizon and VMware Cloud Director , w systemach Kubernetes, systemach operacyjnych Linux i Windows.
21. Rozwiązanie powinno wykrywać zagrożenia bezpieczeństwa i błędy w konfiguracji Jednostki w środowiskach chmurowych AWS, Azure, GCP.
22. Rozwiązanie musi mieć budowę modułową, gdzie funkcjonalności można wdrożyć również oddzielnie dla pojedynczego obszaru technologicznego takiego jak VMware, Kubernetes, systemy operacyjne, środowiska chmurowe AWS, Azure, GCP.
23. Rozwiązanie musi klasyfikować wykryte zagrożenia i podatności na czterech poziomach istotności:
    1. Critical (krytyczne)
    2. Major (główne)
    3. Medium (średnie)
    4. Low (informacyjne)
24. Rozwiązanie musi mieć mechanizm generowania raportów bezpieczeństwa w oparciu o filtry z możliwością eksportu do pliku PDF.
25. Rozwiązanie musi umożliwiać zdalne połącznie (bezagentowe) do analizowanych środowisk:
    1. VMware
    2. Kubernetes
    3. Microsoft Azure
    4. Amazon AWS
    5. Google Cloud Platform
26. Rozwiązanie musi posiadać funkcjonalność zbierania danych w celu analizy zagrożeń i podatności z poziomu systemów operacyjnych.
27. W przypadku stosowania rozwiązania agentowego dla systemów operacyjnych, pliki instalacyjne oprogramowania agenta powinny mieć możliwość przygotowania do automatycznej instalacji z wykorzystaniem systemów dystrybucji oprogramowania np.: GPO dla Windows, Ansible dla Linux.

**II Funkcjonalności modułów rozwiązania:**

**A) Funkcjonalność modułu dedykowanego** **dla środowisk VMware**

1. Funkcjonalność modułu dla środowisk VMware musi analizować środowisko wirtualne VMware (vSphere, vSAN, NSX-V, NSX-T, Horizon, VMware Cloud Director) i wykrywać zagrożenia opisane w Bazie Wiedzy (Knowledge Base) firmy VMware.
2. Funkcjonalność modułu dla VMware musi automatyczne wykrywać podatności bezpieczeństwa dla systemu VMware vSphere, NSX-T, NSX-V i korelować je co najmniej z katalogiem CISA KEV (ang. Known Exploited Vulnerabilities)w celu wskazania zagrożeń o najwyższym priorytecie do rozwiązania.
3. Jeżeli wykryte zagrożenie wymaga pobrania i instalacji poprawki, to jego opis musi zawierać bezpośredni link do tej poprawki w oficjalnych źródłach firmy VMware.
4. Funkcjonalność modułu dla środowisk VMware musi posiadać mechanizm zbieranina i analizowania logów ESX i maszyn VM w celu wykrywania zagrożeń opisanych w Bazie Wiedzy (Knowledge Base) firmy VMware.
5. Funkcjonalność modułu dla środowisk VMware musi badać zgodność konfiguracji środowiska wirtualnego z tzw. „Dobrymi Praktykami” (Best Practices) opublikowanymi przez firmę VMware oraz jej partnerów technologicznych (SAP HANA on vSphere, Pure Storage on vSphere, vSphere on Nutanix).
6. Funkcjonalność modułu dla środowisk VMware musi mieć możliwość zautomatyzowanego przeprowadzania audytów bezpieczeństwa środowiska VMware zgodnie z zaleceniami i standardami takimi jak:
   1. BSI IT- Grundschutz,
   2. CIS Critical Security Controls,
   3. Cyber Essentials,
   4. DISA STIG,
   5. Essential 8,
   6. RODO (GDPR),
   7. HIPAA,
   8. ISO 27001,
   9. NIST,
   10. PCI DSS,
   11. VMware Security Configuration Guide.
7. Funkcjonalność modułu dla środowisk VMware musi mieć możliwość tworzenia własnych profili bezpieczeństwa przez Jednostkę w oparciu o reguły dostarczone przez producenta rozwiązania.

**B) Funkcjonalności modułu dedykowanego dla systemów operacyjnych Windows i Linux**

1. Funkcjonalność modułu dla systemów operacyjnych musi wykrywać podatności bezpieczeństwa i korelować z katalogiem CISA KEV (ang. Known Exploited Vulnerabilities)w celu wskazania zagrożeń o najwyższym priorytecie do rozwiązania dla systemu Windows Server 2008 i nowszych, oraz Linux RedHat 7 i nowszych.
2. Funkcjonalność modułu dla systemów operacyjnych musi mieć możliwość zautomatyzowanego przeprowadzania audytów bezpieczeństwa zgodnych z zaleceniami CIS Critical Security Controls dla systemu Windows Server 2016 i nowszych, oraz Linux RedHat 7 i nowszych.
3. Funkcjonalność modułu dla systemów operacyjnych musi mieć możliwość zautomatyzowanego przeprowadzania audytów bezpieczeństwa zgodnych z zaleceniami BSI IT-Grundschutz dla systemu Windows Server.
4. Funkcjonalność modułu dla systemów operacyjnych musi mieć możliwość zautomatyzowanego przeprowadzania audytów bezpieczeństwa zgodnych co najmniej z zaleceniami DISA STIG, NIST dla systemów Windows Server i Linux RedHat.
5. Funkcjonalność modułu dla systemów operacyjnych musi mieć możliwość zautomatyzowanego przeprowadzania analiz konfiguracji maszyn wirtualnych i porównanie konfiguracji z wybranym serwerem wzorcowym Windows i Linux (ang. Baseline Comparision).

**C) Funkcjonalności modułu dedykowanego dla Kubernetes**

1. Funkcjonalność modułu dla Kubernetes musi automatycznie wykrywać znane podatności i automatycznie korelować je z katalogiem CISA KEV (ang. Known Exploited Vulnerabilities)w celu wskazania zagrożeń o najwyższym priorytecie do rozwiązania.
2. Funkcjonalność modułu dla Kubernetes musi mieć możliwość zautomatyzowanego przeprowadzania audytów bezpieczeństwa zgodnie z zaleceniami:
   1. CIS Benchmarks,
   2. BSI IT-Grundshutz,
   3. CISA Hardening Guide dla Kubernetes.
3. Funkcjonalność modułu dla Kubernetes musi badać zgodności konfiguracji środowiska wirtualnego Kubernetes co najmniej z „Dobrymi Praktykami” (Best Practices) opublikowanymi przez Kubernetes.
4. Funkcjonalność modułu dla Kubernetes musi posiadać możliwość skanowania wzorców kontenerów Kubernetes pod kątem znanych podatności (ang. Image Scanning).

**D) Funkcjonalności modułu dedykowanego dla środowisk chmurowych:**

1. Rozwiązanie powinno umożliwiać korzystanie z funkcjonalności dla środowisk chmurowych niezależnie od poszczególnych jego modułów opisanych w OPZ, poprzez zakup odpowiedniej licencji.
2. Rozwiązanie musi posiadać wbudowany mechanizm do analizy środowisk chmurowych Azure co najmniej pod kątem zgodności z zaleceniami bezpieczeństwa opublikowanymi przez:
   1. BSI IT-Grundschutz.
   2. CIS CSC.
   3. RODO (GDPR).
3. Rozwiązanie musi badać zgodność z zaleceniami bezpieczeństwa dla usług Microsoft Azure takich jak:
   1. AAKS,
   2. Azure AD,
   3. Azure App Services,
   4. Disks, Key Vault,
   5. MySQL Server,
   6. Network Security Group,
   7. Network Watcher,
   8. PostgreSQL Server,
   9. MS SQL Server,
   10. Storage Accounts,
   11. Subscription,
   12. Virtual Machines.
4. Rozwiązanie musi posiadać wbudowany mechanizm do analizy środowisk chmurowych AWS co najmniej pod kątem zgodności z zaleceniami bezpieczeństwa opublikowanymi przez:
   1. CIS CSC.
   2. ISO 27001
   3. NIST
   4. PCI DSS
5. Rozwiązanie musi badać zgodność z zaleceniami bezpieczeństwa dla usług Amazon Web Services takich jak:
   1. AWS Config,
   2. AWS Health,
   3. AWS Inspector,
   4. CloudFront,
   5. CloudTrail,
   6. CloudWatch,
   7. EC2,
   8. ECS,
   9. EFS,
   10. EKS,
   11. IAM,
   12. Kinesis,
   13. Lambda,
   14. RDS,
   15. Redshift,
   16. S3,
   17. VPC.
6. Rozwiązanie musi posiadać wbudowany mechanizm do analizy środowisk chmurowych Google Cloud Platform pod kątem co najmniej zgodności z zaleceniami bezpieczeństwa opublikowanymi przez CIS CSC.
7. Rozwiązanie musi badać zgodność z zaleceniami bezpieczeństwa dla usług Google Cloud Platform takich jak:
   1. Cloud Functions,
   2. Storage Buckets,
   3. DNS Policies,
   4. Firewall Rules,
   5. VPC Networks,
   6. SQL Instances,
   7. Compute Instances,
   8. Service
   9. Accounts,
   10. Metrics & Alerts,
   11. IAM Policies.

**III Usługi Towarzyszące**

**A) Usługi Instalacyjno-Wdrożeniowe**

1. Usługi Instalacyjno-Wdrożeniowe obejmują:
   1. Instalację i konfigurację dostarczonego Oprogramowania przez Wykonawcę,
   2. Wykonanie dokumentacji projektowej, powykonawczej i dokumentacji testów akceptacyjnych,
   3. Instalację Oprogramowania w środowisku Jednostki,
   4. Skonfigurowanie rozwiązania zgodnie z dokumentacją projektową,
   5. Wykonania testów akceptacyjnych wykazujących poprawność wdrożenia rozwiązania zgodnie z dokumentacją projektową.
2. Usługi Instalacyjno-Wdrożeniowe będą realizowane na podstawie zatwierdzonego przez Jednostkę harmonogramu wdrożenia na zasadach określonych w Umowie ramowej.
3. Wykonawca na etapie wdrożenia zapewnieni możliwość udziału osób wskazanych przez Jednostkę przy przeprowadzanym przez inżyniera/inżynierów wdrożeniu rozwiązania po stronie Wykonawcy.
4. Na wniosek Wykonawcy Jednostka może wyrazić zgodę w postaci elektronicznej (e-mail) lub dokumentowej na wykonanie prac instalacyjno-wdrożeniowych zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Wykonawcę. Jednostka ma prawo odmowy udostępnienia zdalnego dostępu w dowolnym momencie bez podawania przyczyny.
5. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Jednostki/Jednostek, w których odbywa się wdrożenie.
6. Jednostka dostarczy uzgodnione z Wykonawcą zasoby informatyczne potrzebne do instalacji i wdrożenia elementów rozwiązania.
7. Wykonawca przeprowadzi, na etapie wdrożenia, warsztaty wdrożeniowe w języku polskim dla maks. 15 uczestników w zakresie obsługi i administracji wdrażanego rozwiązania w wymiarze minimum 16 godzin roboczych w formie zdalnej. Platformę do przeprowadzenia warsztatów zapewni Zamawiający..
8. Warsztaty wdrożeniowe stanowią element usług instalacyjno – wdrożeniowych i polegać będą   
   w szczególności na:
   * 1. udzielaniu odpowiedzi na pytania w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego rozwiązania w środowisku produkcyjnym,
     2. zapewnieniu transferu wiedzy obejmującego swoim zakresem specjalistyczną wiedzę z dostarczanego rozwiązania i przygotowanie uczestników w zakresie administrowania, utrzymania i rozwiązywania problemów.
9. Wykonawca zapewni możliwość konsultowania z trenerami tematów omawianych podczas warsztatów oraz opieki merytorycznej nad uczestnikami warsztatów w okresie 5 dni roboczych po zakończeniu warsztatów za pomocą poczty elektronicznej (udzielanie odpowiedzi drogą elektroniczną na pytania lub wątpliwości powstałe podczas warsztatów).
10. Wszystkie koszty związane z organizacją, przeprowadzeniem, zapewnieniem materiałów szkoleniowych itp. pokrywa Wykonawca.
11. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania rozwiązania będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia zawierający w szczególności:
    1. odbiór prawidłowości wdrożenia i działania rozwiązania na podstawie Dokumentacji Projektowej i przeprowadzonych Testów Akceptacyjnych,
    2. odbiór Dokumentacji Powykonawczej,
    3. odbiór realizacji Warsztatów Wdrożeniowych.

**B) Usługi wsparcia eksperckiego Wykonawcy**

1. Usługi wsparcia eksperckiego Wykonawcy będą obejmowały:
   1. bieżące utrzymanie, zarządzanie i administrowanie oferowanym przez Wykonawcę rozwiązaniem,
   2. przeprowadzenie konsultacji, instruktażu, rozwiązywanie bieżących problemów związanych z obsługą, w tym instalacją, konfiguracją, optymalizacją, utrzymaniem i administracją z wyłączeniem Awarii usuwanych w ramach Gwarancji oraz z wyłączeniem czynności wykonywanych w ramach Wsparcia Technicznego,
2. Rodzaj usługi wsparcia eksperckiego Wykonawcy będzie precyzowany na etapie procedury wykonawczej, z zastrzeżeniem pkt 1 powyżej.
3. Ilości godzin usługi wsparcia eksperckiego Wykonawcy będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług towarzyszących na podstawie ilości godzin wskazanych przez Jednostkę we wniosku o zamówienie.
4. Maksymalna ilość godzin wsparcia eksperckiego w ramach Umowy ramowej wynosi 1000 godzin zegarowych.
5. Godziny wsparcia eksperckiego są uprawnieniem Jednostki, wobec czego Wykonawcy nie przysługuje żadne dodatkowe wynagrodzenie w przypadku niewykorzystania przez Jednostki wszystkich godzin wsparcia eksperckiego w trakcie obowiązywania Umowy ramowej.

**IV Wymagania w zakresie Gwarancji i wsparcia technicznego**

1. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii, oprogramowanie to musi zapewnić Jednostce brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie Awarii.
2. Wszelkie prace wykonywane przez Wykonawcę nie mogą skutkować utratą praw gwarancyjnych.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe Awarii w następujący sposób:
   1. **Awaria Krytyczna**, wada skutkująca nieprawidłowym działaniem dowolnego elementu rozwiązania powodująca albo całkowity brak możliwości korzystania albo takie ograniczenie możliwości korzystania, że rozwiązanie przestaje spełniać swoje podstawowe funkcje. Czas odnalezienia obejścia lub Naprawy do 48 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę;
   2. **Awaria Niekrytyczna** wada skutkująca nieprawidłowym działaniem dowolnego elementu rozwiązania powodująca ograniczenie korzystania z rozwiązania, nie powodując skutków opisanych dla Awarii Krytycznej. Czas odnalezienia obejścia lub Naprawy do 96 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę.
4. Wszelkie Awarie będą zgłaszane przez Jednostkę za pomocą udostępnionej przez Wykonawcę oprogramowania, o którym mowa w punkcie 1 powyżej.
5. W przypadku potrzeby konsultacji z działem wsparcia technicznego Producenta lub wydania poprawki przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Jednostka zawiesi czas usunięcia Awarii do czasu udostępnienia poprawki lecz nie dłużej niż 90 dni.
6. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
7. aktualizację i konfigurację rozwiązania przez Wykonawcę,
8. rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą rozwiązania.
9. Wykonawca w ramach udzielonej gwarancji na wezwanie i w terminie uzgodnionym z Zamawiającym zainstaluje poprawki, usprawnienia i nowe wersje oprogramowania udostępniane przez producenta wdrożonego rozwiązania.
10. W ramach udzielonej gwarancji Jednostce przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji rozwiązania udostępnianych przez jego producenta bez ponoszenia dodatkowych kosztów finansowych przez Jednostkę. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Jednostce.

**V Wymagania w zakresie Dokumentacji Projektowej**

Wykonawca w uzgodnieniu z Jednostką opracuje i dostarczy następującą Dokumentację Projektową:

1. Projekt Wdrożenia, który musi zawierać, w szczególności: opis funkcjonalny, wykaz wymaganych elementów rozwiązania, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania rozwiązania jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Zamawiającego, harmonogram wdrożenia,
2. Dokumentację Testów Akceptacyjnych wdrożenia rozwiązania, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożone rozwiązanie jest zgodne z opisem przedmiotu zamówienia. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Zamawiającego na etapie odbioru Dokumentacji Projektowej.

Dokumentacja musi być dostarczona w wersji elektronicznej i napisana w języku polskim.

Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.

Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu zawierający w szczególności: odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów Akceptacyjnych.

**VI Wymagania w zakresie Dokumentacji Powykonawczej**

Dokumentacja Powykonawcza ma zawierać, w szczególności:

* + - 1. Szczegółową konfiguracją oraz opis infrastruktury technicznej wdrażanego rozwiązania,
      2. Opis struktury i konfiguracji rozwiązania,
      3. Zalecenia i procedury eksploatacyjne oraz zalecenia w zakresie konserwacji rozwiązania,
      4. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji rozwiązania, w szczególności:

1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji,
2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
3. instrukcje dla użytkowników i administratorów,
4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia, uzgodnione z Zamawiającym,

Dokumentacja Powykonawcza powinna być dostarczona w wersji elektronicznej i sporządzona w języku polskim. Procedury i instrukcje Producenta mogą być sporządzone w języku angielskim lub polskim.