Załącznik nr 1 do Umowy nr……z dnia….

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

* dostawa licencji na oprogramowanie wykorzystywane przez Zamawiającego dla 3050 adresów IP wraz z 36 miesięczną subskrypcją i 36 miesięczną gwarancją dla oferowanego rozwiązania zgodnie z wymaganiami określonymi poniżej, albo
* w przypadku zaoferowania rozwiązania równoważnego innego producenta niż rozwiązanie aktualnie wdrożone u Zamawiającego dostawa, uruchomienie i wdrożenie Oprogramowania do skanowania podatności infrastruktury Zamawiającego dla co najmniej 3050 adresów IP wraz z 36 miesięczną licencją i 36 miesięczną gwarancją dla oferowanego rozwiązania równoważnego zgodnego z wymaganiami jak poniżej.

Zamawiający na potrzeby wdrożenia rozwiązania udostępni infrastrukturę niezbędną do uruchomienia maszyn wirtualnych, wg. specyfikacji uzgodnionych z Wykonawcą. Wszystkie czynności związane z wdrożeniem i uruchomieniem Oprogramowania będzie wykonywał Wykonawca. Instalacja i aktualizacja Oprogramowania przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części.

WYMAGANIA DLA DOSTAWY LICENCJI NA OPROGRAMOWANIE WYKORZYSTYWANE PRZEZ ZAMAWIAJĄCEGO

Przedmiotem postępowania jest dostawa licencji na oprogramowanie wykorzystywane przez Zamawiającego wykazane poniżej dla łącznej liczby 3050 adresów IP wraz z 36 miesięczną licencją, w tym w szczególności poszczególnych typów licencji:

1. 50 licencji Tenable.io WAS
2. 3000 licencji Tenable.sc IP

W ramach udzielonej licencji Zamawiający jest uprawnionych do:

1. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
2. dostępu do bazy wiedzy oraz dokumentacji Oprogramowania,

# 1. Środowisko zamawiającego

Zmawiający posada funkcjonujące środowisko, wykorzystujące oprogramowanie:

* Tenable.io WAS,
* T Tenable.sc IP,

# 2. Warunki realizacji zamówienia i gwarancja dla Oprogramowanie

1. Wykonawca udziela Zamawiającemu 36 miesięcznej licencji na dostarczone w ramach umowy Oprogramowanie liczonej od daty podpisania protokołu przedmiotu zamówienia. W ramach udzielonej licencji Zamawiający jest uprawnionych do:
	1. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
	2. dostępu do bazy wiedzy oraz dokumentacji Oprogramowania,
2. Wykonawca udziela gwarancji na wykonane przez Wykonawcę w ramach przedmiotu umowy usługi związane z wdrożeniem Oprogramowania, przez okres 36 miesięcy od dnia podpisania bez zastrzeżeń protokołu odbioru tych prac.

W ramach usług gwarancyjnych Wykonawca ma zagwarantować następujące czasy naprawy Oprogramowania licząc od momentu zgłoszenia przez Zamawiającego:

1. w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Zamawiający definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)
2. w ciągu 72 godzin w przypadku Błędu w Oprogramowaniu (jako Błąd w Oprogramowaniu Zamawiający definiuje nieprawidłowe działanie Oprogramowania lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie Oprogramowania)
3. W ramach udzielonej Zamawiającemu gwarancji awarie lub błędy w funkcjonowaniu Oprogramowania zgłaszane będą drogą telefoniczną lub mailową lub za pomocą systemu udostępnionego przez Zamawiającego po zawarciu umowy.
4. Zamawiający określi drogę dokonywania zgłoszeń serwisowych oraz przygotuje niezbędne dostępy pozwalające na obsługę zgłoszeń.
5. Zamawiający może zawiesić czas naprawy w przypadkach wymagających udzielenia przez producenta Oprogramowania informacji technologicznych niedostępnych w opublikowanych materiałach produktowych oraz w przypadku konieczności interwencji producenta w szczególności polegających na wprowadzaniu zmian takich jak przygotowanie odpowiednich poprawek w produktach. W przypadku wystąpienia opóźnień leżących po stronie producenta Oprogramowania Wykonawca zobowiązany jest poinformować Zamawiającego o zaistniałym fakcie.

WYMAGANIA DLA PRZEDMIOTU ZAMÓWIENIA W PRZYPADKU ZAOFEROWANIA OPROGRAMOWANIA RÓWNOWAŻNEGO

# W przypadku zaoferowania rozwiązania równoważnego innego producenta, przedmiotem postępowania będzie dostawa, uruchomienie i wdrożenie Oprogramowania do skanowania podatności infrastruktury Zamawiającego dla łącznej liczby co najmniej 3000 adresów IP (w tym 50 licencji dla funkcjonalności skanowania web aplikacji) wraz z 36 miesięczną licencją i 36 miesięczną gwarancją dla oferowanego rozwiązania równoważnego zgodnego z wymaganiami jak poniżej. Zamawiający na potrzeby wdrożenia rozwiązania równoważnego udostępni infrastrukturę niezbędną do uruchomienia maszyn virtualnych, wg. specyfikacji uzgodnionych z Wykonawcą. Wszystkie czynności związane z wdrożeniem i uruchomieniem Oprogramowania będzie wykonywał Wykonawca.

# 3. Wymagania funkcjonalne dla oprogramowania równoważnego

1. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.
2. Jeżeli System będzie instalowany jako System na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server oraz Red Hat.
3. Jeżeli System będzie dostępny przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersjach na dzień składania oferty.
4. Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego: Windows 10 i nowszych, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/CentOS/Debian).
5. System musi dawać możliwość skanowania urządzeń końcowych działających na różnych systemach operacyjnych oraz znajdujących się w różnych podsieciach.
6. System (zarówno silnik jak i konsola) powinien dawać możliwość wdrożenia, jako:
	1. aplikacja tj. System instalowany na systemie operacyjnym skanowanego hosta –agent;
	2. maszyna wirtualna;
7. System musi opcjonalnie, w określonych okolicznościach, dawać możliwość zainicjowania skanowania z poziomu: serwera (instalacja standalone), aplikacji dowolnego silnika skanującego (skanera), linii poleceń systemu, w którym jest zainstalowany skaner.
8. System powinien obsługiwać automatyczny i zaplanowany transfer logów z konsoli w celu archiwizacji.
9. Elementy zarządzające i analityczne Systemu nie mogą być ograniczone liczbą skanerów sieciowych w różnych podsieciach, liczbą hostów w podsieci czy liczbą możliwych do skanowania podsieci.
10. Wymagana jest możliwość wykorzystania mechanizmu proxy do komunikacji z Internetem.
11. W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.
12. W przypadku dostępu do Internetu System ma umożliwiać aktualizację automatyczną jak również ręczną z poziomu panelu zarządzania Systemem.
13. W przypadku skanów aplikacji webowych z Internetu Zamawiający dopuszcza możliwość skorzystania z dodatkowych narzędzi np.: dodatkowego panelu zarządzania lub dodatkowego systemu, w tym umiejscowionego w chmurze.
14. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.
15. Dostęp do systemu możliwy jedynie po uwierzytelnieniu użytkownika w systemie.
16. Hasła dostępu muszą być przechowywane w postaci zaszyfrowanej.
17. System musi zapewniać silną politykę haseł lub umożliwiać jej określenie dla użytkowników Systemu.
18. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do raportów, administrator systemu itp.) lub poprzez możliwość przypisania określonych operacji do zdefiniowanych ról.
19. System musi zapewniać segregację obowiązków poprzez umożliwianie dostępu danemu użytkownikowi tylko do wybranych zasobów.
20. System musi się integrować z Active Directory w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.
21. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem wszystkich danych zbieranych przez system.
22. System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli. Dashboard powinien umożliwiać schodzenie do szczegółów w poszczególnych elementów z poziomu informacji podstawowych.
23. System centralnego zarządzania musi zapewnić możliwość:
	1. przechowywania wszystkich danych pochodzących z silnika skanującego i testującego,
	2. przeglądanie tych danych w sposób przejrzysty dla użytkownika, co najmniej w postaci Top 10 podatności, Top 10 systemów zainfekowanych, możliwość filtrowania wykrytych podatności, informacja o połączeniach między systemami klienckimi a serwerami.
	3. tworzenie raportów dostępnych w systemie centralnego zarządzania oraz wysyłanych na wskazane adresy email.
	4. monitorowania stanu pracy skanerów, co najmniej przez: okresową weryfikację czy skanery są uruchomione, stan pracy skanera,
	5. prezentacji informacji o podatnościach wykrytych przez skanery pasywne,
	6. prezentacji wyników skanowania otrzymanych ze skanerów aktywnych,
	7. prezentacji informacji o podatnościach w połączeniu z wynikami skanowania ze skanerów aktywnych.
24. Szyfrowaną komunikację między serwerem zarządzającym a agentem zainstalowanym na stacji roboczej/serwerem.
25. System musi zapewniać możliwość harmonogramowania (planowania w czasie) oraz jednoczesnego uruchomienia na wybranych lub wszystkich skanerach zainstalowanych na stacjach roboczych i serwerach podłączonych do systemu centralnego zarządzania. W tym również w sytuacji, gdy stacja robocza/serwer/skaner na stacji lub serwerze nie jest uruchomiony/-a (uruchomienie jest inicjowane przez system centralnego zarządzania).
26. System musi zapewnić silne uwierzytelnianie tak aby bezpiecznie przesyłać poświadczenia w skanowaniu z uwierzytelnianiem.
27. System musi mieć możliwość wykonywania ręcznego i zaplanowanego skanowania określonych hostów lub podsieci.
28. Wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące muszą być przesyłane niezwłocznie do centralnej bazy i nie mogą być przechowywane przez skaner lokalnie.
29. Skanery aktywne podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego,
30. System powinien zapewnić możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod podczas skanowania z serwera:
	1. Hasło
	2. Klucz SSH
	3. Kerberos, w tym integracja z Microsoft AD oraz Azure AD opcjonalnie możliwość zapewnienia użycia logowania wieloskładnikowego (MFA).
31. System powinien zapewnić możliwość automatyzacji procesów i obejmować co najmniej:
	1. skanowanie o zaplanowanym czasie;
	2. powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport);
	3. możliwość tworzenia okien czasowych, w których skanowanie aktywne nie może rozpocząć się dla określonych przez administratora systemów;
32. System musi umożliwiać automatyczne przeprowadzanie retestów luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.
33. Wykryte podatności powinny posiadać odnośniki do otwartych baz podatności, takich jak:
	1. Bugtraq
	2. MSFT
	3. CVE
	4. BID
	5. OSVDB ID
34. System musi mieć możliwość tworzenia grup dla danych wynikowych.
35. System centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw,
36. W ramach budowy polityki skanowania system musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE
37. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:
	1. Adres IP,
	2. Poziom niebezpieczeństwa,
	3. CVE ID,
	4. CVSS Score w wersji 2 i nowszych,
	5. CVSS Vector w wersji 2 i nowszych,
	6. Dostępny exploit,
	7. narzędzi do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),
	8. data opublikowania patch dla danej podatności,
	9. port/protokół,
	10. data opublikowania podatności,
	11. data zauważenia po raz pierwszy podatności dla systemu,
	12. data, kiedy ostatni raz widziana była podatność dla systemu,
	13. przydział do określonej grupy systemów,
	14. CCE ID,
	15. MS Bulletin ID,
38. System musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego.
39. Administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu.
40. System musi prezentować wyniki skanowania co najmniej za pomocą widoków:
	1. sumarycznie po IP,
	2. sumarycznie po portach,
	3. sumarycznie po grupach systemów,
	4. sumarycznie po CCE,
	5. sumarycznie po CVE,
	6. sumarycznie po MS Bulletin ID,
	7. sumarycznie po protokołach,
	8. sumarycznie po systemach operacyjnych,
41. System musi umożliwiać tworzenie grup systemów spełniających określone warunki. Grupy systemów mogą być tworzone dynamicznie i/lub statycznie. Tworzenie grup powinno być możliwe w oparciu o co najmniej następujące parametry:
	1. system operacyjny,
	2. MAC adres,
	3. IP adres,
	4. porty TCP i UDP,
	5. ilość dni od wykrycia konkretnej podatności,
	6. czy exploit jest dostępny,
	7. czy istnieje exploit w systemach między innymi Metasploit, Core Impact, Canvas,
42. Tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów,
43. Raportowanie musi być integralną częścią systemu centralnego zarządzania,
44. System musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.
45. System musi pozwalać na budowanie raportu od podstaw używając do tego co najmniej elementów takich jak: rozdziały, iteracja wyników, linie trendów, wykresy kołowe, wykresy słupkowe, tabele, macierze, sekcje tekstów.
46. System musi umożliwiać generowane raportów co najmniej w następujących formatach: PDF, CSV.
47. System musi pozwalać na dodanie znaku wodnego podczas generowania raportu,
48. System musi mieć możliwość generowana raportów według harmonogramu oraz na żądanie,
49. System musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila,
50. System musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:
	1. podanie listy adresów IP,
	2. wskazanie zakresu adresów IP,
	3. podanie listy adresów IP podsieci,
	4. tworzenie dynamicznie lub statycznie grup systemów,
	5. wskazanie nazw domenowych systemów.
51. System musi posiadać gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu,
52. Administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak:
	1. tabela,
	2. wykres kołowy,
	3. wykres liniowy,
	4. wykres słupkowy,
	5. macierz (każda komórka oraz nagłówek definiowany oddzielnie),
53. Administrator do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:
	1. adres IP,
	2. Poziom niebezpieczeństwa,
	3. CVE ID,
	4. CVSS Score w wersji 2 i nowsze,
	5. CVSS Vector w wersji 2 i nowsze,
	6. Dostępny exploit,
	7. narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),
	8. data opublikowania patch’a dla danej podatności,
	9. port, protokół,
	10. data opublikowania podatności,
	11. data pierwszy raz zauważenia podatności dla systemu,
	12. data, kiedy ostatni raz widziana była podatność dla systemu,
	13. przyodział do określonej grupy systemów,
	14. CCE ID,
	15. MS Bulletin ID,
54. System musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA.
55. System musi umożliwiać tworzenie swoich własnych wzorców sprawdzania zgodności bez konieczności kontaktu z suportem producenta. Producent musi udostępniać informację w jaki sposób można budować swoje własne wzorca sprawdzania zgodności ze standardami przyjętymi w firmie,
56. System musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów:
	1. Windows,
	2. Unix,
	3. Vmware,
	4. Cisco,
	5. Fortigate,
	6. Oracle,
	7. MySQL,
	8. SQL Server,
	9. PostgreSQL,
	10. Juniper.
57. System powinien umożliwiać ciągłe monitorowanie ruchu w sieci w celu wykrycia podejrzanych przepływów sieciowych z lub do podatnych usług, nieznanych urządzeń, botnetów lub serwerów Command and Control (tzw. C&C).
58. System powinien oferować szablony wzorców zgodności z regulacjami takimi jak: CERT, STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH.
59. System powinien oferować możliwość integracji z systemami firm trzecich do zarządzania aktualizacjami.
60. Oferowany system musi mieć funkcjonalność analizy ruchu sieciowego tzw. skaner pasywny która musi:
	1. umożliwiać zdefiniowanie adresów IP stacji roboczych/serwerów/sieci, które będą podlegać monitorowaniu.
	2. wykrywać nowo pojawiąjące się stacje robocze/serwery w monitorowanej sieci i informować o tym system centralnego zarządzania.
	3. zapewnić monitorowanie sieci lokalnej przez 24 godziny i 7 dni w tygodniu, z minimalnym czasem pracy 95% w skali roku, co najmniej w zakresie wykrywania zagrożeń, anomalii w sieci.
	4. pozwalać na import pliku typu pcap w celu jego analizy – ręczny oraz przez system centralnego zarządzania.
	5. umożliwiać wysyłanie logu systemu w formacie CEF.
	6. umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu.

# 4. Wdrożenie Oprogramowania równoważnego

1. W przypadku zaoferowania innego rozwiązania niż obecnie wykorzystywane przez Zamawiającego tj. Tenable.sc IP i Tenable.io WAS, Wykonawca w terminie do 14 dni kalendarzowych od daty podpisania umowy będzie odpowiedzialny za dostarczenie, instalację i konfigurację środowiska Systemu w infrastrukturze Zamawiającego. Wykonawca dodatkowo zobowiązany jest do przeniesienia konfiguracji i wykonania testów potwierdzających prawidłowość odwzorowania konfiguracji w nowym środowisku.
2. Wykonawca dostarczy projekt techniczny zawierający w szczególności:
	1. Plan i opis architektury logicznej Oprogramowania
	2. Opis funkcji Oprogramowania do zaimplementowania w infrastrukturze Zamawiającego w szczególności szczegółowy opis zakresu integracji Oprogramowania z infrastrukturą Zamawiającego.
	3. Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca)

niezbędnych do dostosowania Oprogramowania do potrzeb Zamawiającego i konfiguracji środowiska produkcyjnego.

* 1. Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego.
1. W przypadku zaoferowania innego rozwiązania niż obecnie wykorzystywane przez Zamawiającego tj. Tenable.sc IP i Tenable.io WAS, Wykonawca wykona prace implementacyjno-wdrożeniowe obejmujące co najmniej:
	1. wykonanie analizy technicznej i przygotowania projektu technicznego wdrożenia,
	2. Instalacja i konfiguracja rozwiązania,
	3. Konfiguracja i integracja z Active Directory, serwerem DHCP, DNS,
	4. Przeniesienie ustawień konfiguracyjnych z istniejącego środowiska Zamawiającego (użytkowników i ich uprawnień, szablonów raportów, szablonów skanowania, zapisanych poświadczeń, konfiguracji grup skanowania, Harmonogramów skanowania itp.)
	5. Przygotowanie min. Trzech skanów podatności i trzech testów aplikacji oraz uruchomienie ich.
	6. Przeprowadzenie strojenia samego Oprogramowania oraz doboru odpowiednich parametrów celem otrzymania najwydajniejszej i najbardziej bezpiecznej konfiguracji Oprogramowania,
	7. Przeprowadzanie prac optymalizacji Oprogramowania pod kątem minimalizacji liczby fałszywych alertów.
	8. Projekt techniczny zostanie wykonany w formie elektronicznej w zgodniej z formatem z .doc lub .pdf

# 5. Dokumentacja powykonawcza systemu równoważnego

1. Wykonawca opracuje i dostarczy Zamawiającemu w formie elektronicznej zgodnej z formatem z .doc lub .pdf dokument „Dokumentacja powykonawcza".
2. Dokumentacja powykonawcza powinna zawierać następujące elementy:
	1. Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Oprogramowania
	2. Architektura logiczna Oprogramowania (graficzna prezentacja Oprogramowania i jego połączeń wraz z opisem)
	3. Przepływ danych w Oprogramowaniu (koncepcja obiegu informacji w systemie pomiędzy poszczególnymi komponentami, warstwami Oprogramowania)
	4. Szczegółowa konfiguracja poszczególnych elementów Oprogramowania (np. serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www - zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji Oprogramowania)
	5. Polityka aktualizacji Oprogramowania i testowania zmian
	6. Architektura sieciowa Oprogramowania (opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów Oprogramowania w poszczególnych strefach - DMZ, LAN, Internet)
	7. Opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów)
	8. Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w Oprogramowaniu)
	9. Procedura odtwarzania Oprogramowania (opisanie procedury backupu i odtworzenia całego Oprogramowania i jego poszczególnych elementów, opis procedur przywracania Oprogramowania do pełnej funkcjonalności po awarii)
	10. Procedura instalacji Oprogramowania (opis procedury instalacji Oprogramowania „od początku - krok po kroku", opis wszystkich kroków instalacji i konfiguracji Oprogramowania w postaci zrzutów ekranu z opisami),
	11. Procedury wykonywania krytycznych operacji w Oprogramowaniu (migracja, aktualizacja),
	12. Instrukcje obsługi Oprogramowania dla Administratorów.

# 6. Instruktaż stanowiskowy dla wdrożonego Oprogramowania równoważnego

Instruktaż stanowiskowy musi obejmować wszystkie zagadnienia i musi odpowiadać wersji wdrożonego u Zamawiającego Oprogramowania:

1. instalacja i konfiguracja wszystkich modułów Oprogramowania,
2. praktyczne wykorzystanie zaimplementowanych funkcjonalności oprogramowania:
	* 1. tworzenie i zarządzanie zadaniami oraz politykami skanowania,
		2. praktyczne przeprowadzenie różnych rodzajów skanowania, w tym w oparciu o skonfigurowane polityki skanowania,
		3. konfiguracja funkcji badania zgodności, praktyczne przeprowadzenie audytów zgodności,
		4. interpretacja wyników skanowania/audytowania, analiza ryzyka,
		5. konfiguracja funkcji raportowania, generowania raportów,
		6. tworzenie i zarządzanie szablonami raportów,
3. Opis i przedstawienie integracji Oprogramowania z usługami Zamawiającego,
4. Zarządzanie wdrożonym Oprogramowaniem:
	* 1. możliwości rozbudowy, przyłączani, odłączanie i konfigurowanie poszczególnych modułów skanujących,
		2. rozwiązywanie problemów powstałych w procesie zarządzania podatnościami,
		3. wykonywanie czynności administracyjnych oraz zadań dotyczących utrzymania wdrożonego oprogramowania.
5. Zasady realizacji instruktażu stanowiskowego:
	1. dla maksimum 6 osób wskazanych przez Zamawiającego
	2. łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 2 dni robocze Zamawiającego.
	3. instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
	4. instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Oprogramowania,
	5. instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych Zamawiającego, tj. pn – pt, w godzinach 8:15 – 16:15
	6. Osoby prowadzące instruktaż stanowiskowy muszą posiadać wiedzę oraz odpowiednie przygotowanie merytoryczne w zakresie wdrażanego Oprogramowania, a także brać bezpośredni udział we wdrożeniu tego Oprogramowania.
6. W ramach realizacji instruktażu stanowiskowego Wykonawca zapewni każdemu uczestnikowi materiały dydaktyczne w języku polskim lub angielskim (w formie elektronicznej), co najmniej:
	1. podręcznik administratora i użytkownika w formie elektronicznej,
	2. szczegółowy plan zajęć,
	3. opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji Oprogramowania.

# 7 Warunki realizacji zamówienia i gwarancja dla Oprogramowania równoważnego

1. Wykonawca udziela Zamawiającemu 36 miesięcznej licencji na dostarczone w ramach umowy Oprogramowanie liczonej od daty podpisania protokołu odbioru przedmiotu zamówienia. W ramach udzielonej licencji Zamawiający jest uprawnionych do:
	1. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
	2. dostępu do bazy wiedzy oraz dokumentacji Oprogramowania,
2. Wykonawca udziela gwarancji na wykonane przez Wykonawcę w ramach przedmiotu umowy usługi związane z wdrożeniem Oprogramowania, przez okres 36 miesięcy od dnia podpisania bez zastrzeżeń protokołu odbioru tych prac.

W ramach usług gwarancyjnych Wykonawca ma zagwarantować następujące czasy naprawy Oprogramowania licząc od momentu zgłoszenia przez Zamawiającego:

* 1. w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Zamawiający definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)
	2. w ciągu 72 godzin w przypadku Błędu w Oprogramowaniu (jako Błąd w Oprogramowaniu Zamawiający definiuje nieprawidłowe działanie Oprogramowania lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie Oprogramowania)
1. W ramach udzielonej Zamawiającemu gwarancji awarie lub błędy w funkcjonowaniu Oprogramowania zgłaszane będą drogą telefoniczną lub mailową lub za pomocą systemu udostępnionego przez Wykonawcę po zawarciu umowy. Po każdym zgłoszeniu awarii lub błędu Wykonawca jest zobowiązany do potwierdzenia otrzymania zgłoszenia od Zamawiającego.
2. Wykonawca określi drogę dokonywania zgłoszeń serwisowych oraz przygotuje niezbędne dostępy pozwalające na dokonanie zgłoszenia przez pracowników Zamawiającego. Wykonawca będzie prowadził całą historię złożonych zleceń oraz zapewni Zamawiającemu wgląd do systemu zawierający opis wszystkich zgłoszeń w całym okresie realizacji umowy. Wykonawca zapewni Zamawiającemu możliwość dokonywania zgłoszeń w trybie 24/7. Każde zgłoszenie złożone przez Zamawiającego powinno zawierać:
	1. datę i godzinę zgłoszenia
	2. opis Awarii lub Błędu
	3. sposób naprawy oraz czas realizacji zlecenia.
3. Zamawiający może zawiesić czas naprawy w przypadkach wymagających udzielenia przez producenta Oprogramowania informacji technologicznych niedostępnych w opublikowanych materiałach produktowych oraz w przypadku konieczności interwencji producenta w szczególności polegających na wprowadzaniu zmian takich jak przygotowanie odpowiednich poprawek w produktach. W przypadku wystąpienia opóźnień leżących po stronie producenta Oprogramowania Wykonawca zobowiązany jest poinformować Zamawiającego o zaistniałym fakcie.