Załącznik nr 1 do Umowy nr……z dnia….

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

- dostawa licencji na oprogramowanie wykorzystywane przez Zamawiającego dla co najmniej 3000 adresów IP wraz z 36 miesięczną subskrybcją 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 3000 adresów IP wraz z 36 miesięczną licencją i 36 miesięczną gwarancją dla oferowanego rozwiązania równoważnego zgodnego z wymaganiami jak poniżej.

Instalacja i aktualizacja Oprogramowania przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części.

I. WYMAGANIA DLA DOSTAWY LICENCJI NA OPROGRAMOWANIE WYKORZYSTYWANE PRZEZ ZAMAWIAJĄCEGO:

Przedmiotem postępowania jest dostawa licencji na oprogramowanie wykorzystywane przez Zamawiającego wykazane poniżej dla łącznej liczby co najmniej 3000 adresów IP wraz z 36 miesięczną licencją, w tym w szczególności poszczególnych typów licencji:

a) 100 licencji Tebable.io Web Application Scanning
b) 2900 licencji Tenable.sc Continuous View

W ramach udzielonej licencji Zamawiający jest uprawnionych do:

a) bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
b) dostępu do bazy wiedzy oraz dokumentacji Oprogramowania,

1. Środowisko zamawiającego

Zmawiający posada funkcjonujące środowisko, wykorzystujące oprogramowanie:

- Tenable.sc Continuous View (TE-TSCCV),
- Tebable.io Web Application Scanning (TE-TIO-WAS),

2. Warunki realizacji zamówienia i gwarancja dla Oprogramowania

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:

a. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
b. 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:

a. w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Zamawiający definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)
b. 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 Wykonawcę po zawarciu umowy. Po każdym zgłoszeniu awarii lub błędu Wykonawca jest zobowiązany do potwierdzenia otrzymania zgłoszenia od Zamawiającego.

4) 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:

a. datę i godzinę zgłoszenia
b. opis Awarii lub Błędu
c. sposób naprawy oraz czas realizacji zlecenia.

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.

II. 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 100 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.

1. Wymagania funkcjonalne

2. Zarządzanie Oprogramowaniem musi się odbywać przy pomocy przeglądarki, nie dopuszcza się zarządzania za pomocą dodatkowo instalowanej aplikacji na komputerze administratora,
3. architektura Oprogramowania musi składać się z systemu centralnego zarządzania oraz skanerów podłączonych do tego systemu pochodzących od tego samego producenta co system centralnego zarządzania,
4. Skanowanie może być wykonywane z poziomu: serwera (instalacja stand – alone), dowolnego silnika skanującego, chmury,
5. Oprogramowanie musi być zaimplementowane w infrastrukturze Zamawiającego,
6. Oprogramowanie (zarówno silnik jak i konsola) powinno dawać możliwość wdrożenia, jako:
   6.1. aplikacja tj. oprogramowanie instalowane na systemie operacyjnym skanowanego hosta,
   6.2. maszyna wirtualna,
   6.3. oprogramowanie w chmurze,
   6.4. wszystkie wyżej wymienione sposoby wdrożenia powinny mieć możliwość jednoczesnego uruchomienia w całym środowisku,
7. Oprogramowanie powinno mieć możliwość pracy w modelu hybrydowym,
8. System centralnego zarządzania powinien dawać możliwość:
   8.1. przechowywania wszystkich danych pochodzących z dowolnego silnika skanującego i testującego,
   8.2. wszystkie dane zebrane przez zewnętrzne silniki skanujące i testujące powinny być przesyłane do centralnej bazy i nie powinny być przechowywane po stronie silników skanujących,
   8.3. podłączenia nieograniczonej liczby skanerów aktywnych oraz skanerów pasywnych o interfejsach monitorujących wyposażonych interface 1 Gbit/s,
9. Oprogramowanie musi otrzymywać od producenta informacje o niebezpiecznych adresach IP oraz domenach w celu wykrycia czy systemy, które kontrolowane są przez system zarządzania podatnościami nie łączą się z nimi,
10. skanery aktywne podłączone do systemu centralnego zarządzania muszą mieć możliwość wykonywania skanowania bez uwierzytelnienia oraz za pomocą uwierzytelnienia do systemu skanowanego,
11. w ramach skanowania z uwierzytelnieniem musi istnieć możliwość uwierzytelnienia przynajmniej za pomocą poniższych metod:
    11.1. -Hasło
    11.2. - Klucz SSH
    11.3. - Kerberos,
    11.4. - LM Hash
    11.5. - NTLM Hash
    11.6. - zastosowanie integracji z Liberman
    11.7. - zastosowanie integracji z BeyondTrust
    11.8. - zastosowanie integracji z LibermanThycotic Secret Server
    11.9. - zastosowanie integracji z Cyberark
    11.10. - Certyfikat
    11.11. - DB2
    11.12. - File Transfer Protocol (FTP)
    11.13. - Microsoft SQL Server

11.14. - MySQL Server
11.15. - Oracle
11.16. - Post Office Protocol (POP)
11.17. - PostgreSQL
11.18. - Simple Network Management Protocol (SNMP)
11.19. - Informix

12. Oprogramowanie powinno wspierać poniżej wymienione mechanizmy autentykacji:
    12.1. Simple Form Auth
    12.2. HTTP Auth (Basic, Digest, NTLM)
    12.3. Selenium
13. w przypadku niektórych metod uwierzytelnienia do systemu skanowanego musi istnieć możliwość automatycznego podniesienia uprawnień zwykłego użytkownika do uprawnień użytkownika uprzywilejowanego co najmniej dla systemów Cisco oraz systemów Linuxowych,
14. Oprogramowanie zarządzające musi wspierać minimum systemy operacyjne:
    14.1. Red Hat Enterprise Linux 5.x, i nowsze,
    14.2. Centos,
    14.3. Virtualized Machines on VMware ESXi 5.x i nowsze,
    14.4. VMware vCenter Server 4.x i nowsze,
    14.5. Maszyny wirtualne na Hyper-V 2012 i nowsze,
15. Skanery pasywne oraz aktywne musi wspierać systemy operacyjne:
    15.1. Linux
    15.2. Windows
    15.3. MacOS
16. skanery pasywne muszą działać w oparciu o kopie ruchu dostarczaną za pomocą Span portów lub tapów, aby w żaden sposób nie blokowały lub zmieniały ruchu produkcyjnego
17. skaner pasywny musi mieć możliwość dostarczenia jako obraz Vmware lub jako oprogramowanie instalowane na systemach Windows, Rad Hat lub MAC OS.
18. skaner pasywny musi wykryte informacje o podatnościach przesyłać do systemu centralnego zarzadzania w celu wizualizacji ich wraz z wynikami ze skanowania za pomocą skanerów aktywnych,
19. skaner pasywny musi posiadać również swój własny interfejs webowy w którym posiada miedzy innymi widoki Top 10 podatności, Top 10 systemów zainfekowanych, możliwość filtrowania wykrytych podatności, informacja o połączeniach między systemami klienckimi a serwerami,
20. skaner pasywny musi umożliwiać zdefiniowanie adresów IP, sieci, które będą podlegać monitorowaniu,
21. skaner pasywny musi wykrywać nowo pojawiające się systemy w monitorowanej sieci,
22. skaner pasywny musi monitorować sieć 24 godziny 7 dni w tygodniu,
23. skaner pasywny musi pozwalać na ręczny import pliku typu pcap w celu jego analizy,
24. skaner pasywny musi umożliwiać wysyłanie sysloga w formacie CEF,
25. skaner pasywny musi umożliwiać tworzenie własnych reguł służących do wykrywania określonych elementów w monitorowanym ruchu.
26. automatyzacja procesów, powinna obejmować co najmniej:
    - skanowanie o zaplanowanym czasie
    - powiadamianie i alarmowanie administratora o zdefiniowanych zdarzeniach (np. syslog, SMTP, uruchom skan, wygeneruj raport)
    - możliwość tworzenia okien czasowych, w których skanowanie aktywne nie może rozpocząć się dla określonych przez administratora systemów
27. Oprogramowanie musi umożliwiać skanowanie systemów pod kontem malware.
28. Wszystkie testy i skany, które mogą wpłynąć na stabilność działania sprawdzanego hosta, powinny być oznaczone w jasny sposób dla administratora,
29. Oprogramowanie powinno wspierać poniższe opcje konfiguracji skanowania:

29.1. Attack Policy
29.2. Authentication
29.3. Crawler Restrictions
29.4. HTTP Headers
29.5. Performance
29.6. Selenium Recordings
29.7. Custom URLs
29.8. Advanced Options

30. Oprogramowanie powinno umożliwiać przeprowadzanie tzw. Retestów wobec pojedynczych luk/podatności wykrytych wcześniej w celu sprawdzenia czy zostały one poddane działaniem naprawczym.
31. wykryte podatności powinny posiadać szybkie odniesienie do otwartych baz podatności, takich jak:
    31.1. Bugtraq
    31.2. MSFT
    31.3. CVE
    31.4. BID
    31.5. OSVDB ID
32. Oprogramowanie musi posiadać możliwość tworzenia odseparowanych przestrzeni w bazie systemu zarządzania podatnościami w których przetrzymywane są wyniki skanowania z różnych skanowań, (np. wyniki skanowania sieci A przetrzymywane w osobnej przestrzeni niż wyniki skanowania sieci B),
33. administrator musi mieć możliwość definiowania do jakiej części bazy systemu centralnego zarządzenia przesyłane są wyniki skanowania,
34. Oprogramowanie musi mieć możliwość tworzenia wielu organizacji w ramach jednego systemu centralnego zarządzania,
35. administrator musi mieć możliwość definiowania do jakich organizacji przypisane są poszczególne przestrzenie z bazy danych do przechowywania wyników skanowania,
36. poszczególne organizacje w ramach jednego systemu centralnego zarządzania muszą mieć opcję widzenia lub nie wyników z innych organizacji w zależności od konfiguracji systemu,
37. system centralnego zarządzania musi dostarczać wzorce polityk skanowania jak również możliwość zbudowania polityki skanowania od podstaw,
38. w ramach budowy polityki skanowania system musi zezwalać na wybranie podatności jakie będą sprawdzane podczas skanowania, np. w oparciu o CVSS lub CVE
39. Musi istnieć możliwość przeszukiwania wyników co najmniej za pomocą filtrów takich jak:
    39.1. Adres IP,
    39.2. Poziom niebezpieczeństwa,
    39.3. CVE ID,
    39.4. CVSS Score w wersji 2 i nowszych,
    39.5. CVSS Vector w wersji 2 i nowszych,
    39.6. Dostępny exploit,
    39.7. narzędzi do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),
    39.8. data opublikowania patch dla danej podatności,
    39.9. port, protokół,
    39.10. data opublikowania podatności,
    39.11. data zauważenia po raz pierwszy podatności dla systemu,
    39.12. data kiedy ostatni raz widziana była podatność dla systemu,
    39.13. przydział do określonej grupy systemów,
    39.14. CCE ID,
    39.15. MS Bulletin ID,
40. Oprogramowanie musi posiadać swój własny mechanizm przyznawania ocen dla danej podatności (np. od 0 do 10) na podstawie własnego modelu uczenia maszynowego,

41. administrator musi mieć możliwość zaakceptowania danego ryzyka oraz zmiany poziomu niebezpieczeństwa związanego z daną podatnością dla konkretnego systemu, portu, protokołu,
42. Oprogramowanie musi prezentować wyniki skanowania co najmniej za pomocą widoków:
    42.1. sumarycznie po IP,
    42.2. sumarycznie po portach,
    42.3. sumarycznie po grupach systemów,
    42.4. sumarycznie po CCE,
    42.5. sumarycznie po CVE,
    42.6. sumarycznie po MS Bulletin ID,
    42.7. sumarycznie po protokołach,
    42.8. sumarycznie po systemach operacyjnych,
43. Oprogramowanie musi umożliwiać tworzenie wielu użytkowników,
44. Oprogramowanie musi umożliwiać tworzenie ról przypisanych do użytkowników,
45. Oprogramowanie 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:
    45.1. system operacyjny,
    45.2. MAC adres,
    45.3. IP adres,
    45.4. porty TCP i UDP,
    45.5. ilość dni od wykrycia konkretnej podatności,
    45.6. czy exploit jest dostępny,
    45.7. czy istnieje exploit w systemach między innymi Metasploit, Core Impact, Canvas,
46. tworzenie nowych grup systemów musi odbywać się również na podstawie wyrażeń logicznych takich jak AND, OR, NOT pomiędzy istniejącymi grupami systemów,
47. Raportowanie musi być integralną częścią systemu centralnego zarządzania,
48. Oprogramowanie musi posiadać gotowe grupy wzorców raportów udostępnionych przez producenta, które administrator może edytować.
49. Oprogramowanie 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, itp.
50. Oprogramowanie musi umożliwiać generowane raportów co najmniej w następujących formatach: PDF, CSV, RTF, CyberScope, DISA ASR, DISA ARF,
51. Oprogramowanie musi pozwalać na dodanie znaku wodnego podczas generowania raportu,
52. Oprogramowanie musi mieć możliwość generowana raportów według harmonogramu oraz na żądanie,
53. Oprogramowanie musi mieć możliwość automatycznego wysyłania raportów do wskazanych osób na maila,
54. Oprogramowanie musi mieć możliwość wyboru systemów do skanowania w oparciu o przynajmniej następujące możliwości:
    54.1. podanie adresów IP,
    54.2. zakresu adresów IP,
    54.3. podsieci adresów IP,
    54.4. grup systemów tworzonych dynamicznie lub statycznie,
    54.5. nazw domenowych,
55. Oprogramowanie musi posiadać gotowe wzorce widoków (ang. Dashboard) do systemu centralnego zarządzania podatnościami, które mogą być edytowane przez administratora systemu,
56. administrator musi mieć możliwość tworzenia widoków od podstaw używając co najmniej takich elementów jak:
    56.1. tabela,

56.2. wykres kołowy,
56.3. wykres liniowy,
56.4. wykres słupkowy,
56.5. macierz (każda komórka oraz nagłówek definiowany oddzielnie),

57. administrator do tworzenia widoków musi mieć możliwość używania co najmniej wymienionych filtrów:
    57.1. adres IP,
    57.2. Poziom niebezpieczeństwa,
    57.3. CVE ID,
    57.4. CVSS Score w wersji 2 i nowsze,
    57.5. CVSS Vector w wersji 2 i nowsze,
    57.6. Dostępny exploit,
    57.7. narzędzie do wykonania ataku (musi istnieć obsługa przynajmniej dla trzech narzędzi, np. Metasploit, Core Impact, Canvas),
    57.8. data opublikowania patch dla danej podatności,
    57.9. port, protokół,
    57.10. data opublikowania podatności,
    57.11. data pierwszy raz zauważenia podatności dla systemu,
    57.12. data kiedy ostatni raz widziana była podatność dla systemu,
    57.13. przyodział do określonej grupy systemów,
    57.14. CCE ID,
    57.15. MS Bulletin ID,
58. Oprogramowanie musi integrować się z zewnętrznymi dostawcami systemów MDM co najmniej:
    58.1. ActiveSync,
    58.2. Apple Profile Manager,
    58.3. Mobile Iron,
    58.4. Microsoft Intune
59. Oprogramowanie musi integrować się systemami zarządzania aktualizacjami w celu sprawdzenia czy wynik ze skanowania pokrywa się z informacjami z tych systemów co najmniej z takimi systemami jak:
    59.1. Microsoft SCCM,
    59.2. Microsoft WSUS,
    59.3. Red Hat Satellite Server,
60. Oprogramowanie musi posiadać wzorce zgodności z regulacjami, które dostarcza producent, co najmniej dla regulacji CIS, DISA,
61. Oprogramowanie 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,
62. Oprogramowanie musi umożliwiać wykonywanie skanów audytowych/konfiguracji co najmniej dla systemów:
    62.1. Windows,
    62.2. Unix,
    62.3. Vmware,`
    62.4. Cisco,
    62.5. Fortigate,
    62.6. Oracle,
    62.7. IBM DB2,
    62.8. MySQL,
    62.9. SQL Server,

62.10. PostgreSQL,
62.11. Juniper,

63. funkcjonalność kontroli aplikacji powinna być standardową częścią rozwiązania a skanowanie powinno zawierać testy sprawdzające (co najmniej OWASP)

1. Wdrożenie Oprogramowania równoważnego

1. Wykonawca w terminie do 30 dni kalendarzowych od daty podpisania umowy będzie odpowiedzialny za dostarczenie, instalację i konfigurację środowiska Systemu w infrastrukturze Zamawiającego.
2. Wykonawca przedstawi Zamawiającemu w terminie do 30 dni kalendarzowych od dnia udostępnienia przez Zamawiającego poprawnie skonfigurowanej infrastruktury pod wdrożenie Oprogramowania 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.
   4) Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Zamawiającego.
3. 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.
   4. Projekt techniczny zostanie wykonany w formie elektronicznej w zgodniej z formatem z .doc lub .pdf.

2. Dokumentacja powykonawcza systemu równoważnego

1. Wykonawca opracuje i dostarczy Zamawiającemu w terminie do od dnia udostępnienia przez Zamawiającego poprawnie skonfigurowanej infrastruktury pod wdrożenie Oprogramowania w formie elektronicznej zgodnej z formatem z .doc lub .pdf dokument „Dokumentacja powykonawcza".
2. Dokumentacja powykonawcza powinna zawierać następujące elementy:
   1) Ogólny opis Oprogramowania
   2) Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Oprogramowania

3) Architektura logiczna Oprogramowania (graficzna prezentacja Oprogramowania i jego połączeń wraz z opisem)
4) Przepływ danych w Oprogramowaniu (koncepcja obiegu informacji w systemie pomiędzy poszczególnymi komponentami, warstwami Oprogramowania)
5) 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)
6) Polityka aktualizacji Oprogramowania i testowania zmian
7) Systemy zależne (np. agenci na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z Oprogramowanniem, opis integracji z innymi usługami w tym w szczególności z MS Active Directory oraz MS Exchange, DHCP, DNS).
8) Specyfikacja i konfiguracja serwerów wirtualnych
9) Architektura sieciowa Oprogramowania (opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów Oprogramowania w poszczególnych strefach - DMZ, LAN, Internet)
10) Opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów)
11) Rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w Oprogramowaniu)
12) Zarządzanie hasłami (opis sposobu przechowywania haseł w Oprogramowanniu, mechanizmów kryptograficznych wykorzystywanych do ich zabezpieczenia, informacje o przechowywaniu haseł w kodzie programu)
13) Uprawnienia kont serwisowych
14) Role administracyjne
15) Ustawienia polityki haseł
16) Procedury zmiany haseł serwisowych, administracyjnych i użytkownika
17) Procedury weryfikacji uprawnień
18) Konfiguracja reguł firewall
19) Bezpieczeństwo transmisji (opis rozwiązań w zakresie zapewnienia poufności transmisji danych zarówno w sieci LAN/DMZ jak i Internet)
20) Ochrona konfiguracji Oprogramowania (ochrona krytycznych plików konfiguracyjnych)
21) Opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w Oprogramowaniu, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury)
22) Ochrona dzienników (opis sposobu zabezpieczenia zapisów w logach przed ich utratą oraz nieuprawnioną zmianą, informacja o czasie przechowywania logów, możliwości przekazania logów do systemów zewnętrznych)
23) Procedura odtwarzania Oprogramowania (opisanie procedury backupu i odtworzenia całego Oprogramowania i jego poszczególnych elementów, określenie czasu potrzebnego na

odtworzenie całego Oprogramowania oraz jego poszczególnych elementów, opis procedur przywracania Oprogramowania do pełnej funkcjonalności po awarii)

24) 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),
25) Procedury wykonywania krytycznych operacji w Oprogramowaniu (migracja, aktualizacja, itp.)
26) Instrukcje obsługi Oprogramowania dla Administratorów.

3. Instruktaż stanowiskowy dla wdrożonego Oprogramowania równoważnego

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

1. instalacja i konfiguracja wszystkich modułów Oprogramowania,
2. praktyczne wykorzystanie zaimplementowanych funkcjonalności oprogramowania:
    a. tworzenie i zarządzanie zadaniami oraz politykami skanowania,
    b. praktyczne przeprowadzenie różnych rodzajów skanowania, w tym w oparciu o skonfigurowane polityki skanowania,
    c. konfiguracja funkcji badania zgodności, praktyczne przeprowadzenie audytów zgodności,
    d. interpretacja wyników skanowania/audytowania, analiza ryzyka,
    e. konfiguracja funkcji raportowania, generowania raportów,
    f. tworzenie i zarządzanie szablonami raportów,
3. Opis i przedstawienie integracji Oprogramowania z usługami Zamawiającego,
4. Zarządzanie wdrożonym Oprogramowaniem:
    a. możliwości rozbudowy, przyłączani, odłączanie i konfigurowanie poszczególnych modułów skanujących,
    b. rozwiązywanie problemów powstałych w procesie zarządzania podatnościami,
    c. wykonywanie czynności administracyjnych oraz zadań dotyczących utrzymania wdrożonego oprogramowania.
5. Zasady realizacji instruktażu stanowiskowego:

    a) dla maksimum 6 osób wskazanych przez Zamawiającego
    b) łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 2 dni robocze Zamawiającego.
    c) instruktaż stanowiskowy będzie prowadzony w siedzibie Zamawiającego lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Zamawiającego
    d) instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Oprogramowania,
    e) instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych Zamawiającego, tj. pn – pt, w godzinach 8:15 – 16:15
    f) Instruktaż stanowiskowy musi zakończyć się w terminie do 30 dni kalendarzowych od dnia udostępnienia przez Zamawiającego poprawnie skonfigurowanej infrastruktury pod wdrożenie Oprogramowania.

g) 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:
   a) podręcznik administratora i użytkownika w formie elektronicznej,
   a) szczegółowy plan zajęć,
   b) opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji Oprogramowania.

III. 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:
   a. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
   b. 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:
   a. w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Zamawiający definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)
   b. 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 Wykonawcę po zawarciu umowy. Po każdym zgłoszeniu awarii lub błędu Wykonawca jest zobowiązany do potwierdzenia otrzymania zgłoszenia od Zamawiającego.
4. 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:
   a. datę i godzinę zgłoszenia
   b. opis Awarii lub Błędu

c. sposób naprawy oraz czas realizacji zlecenia.

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.

IV. Warunki realizacji zamówienia i gwarancja dla Oprogramowania dostarczonego w ramach prawa opcji

1. Wykonawca udziela Zamawiającemu odpowiednio 36 miesięcznej (dla Wariantu I) albo 24 miesięcznej (dla Wariantu II) albo 12 miesięcznej (dla Wariantu III) licencji na dostarczone w ramach umowy Oprogramowanie liczonej od daty podpisania protokołu przedmiotu zamówienia. W ramach udzielonej licencji Zamawiający jest uprawnionych do:

a. bezpłatnego dostępu do wszystkich aktualizacji, poprawek i nowych wersji/kompilacji dostarczonego w ramach umowy Oprogramowania,
b. 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 odpowiednio 36 miesięcy (dla Wariantu I) albo 24 miesięcy (dla wariantu II) albo 12 miesięcy (dla Wariantu I) 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:

a. w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Zamawiający definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)
b. 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 Wykonawcę po zawarciu umowy. Po każdym zgłoszeniu awarii lub błędu Wykonawca jest zobowiązany do potwierdzenia otrzymania zgłoszenia od Zamawiającego.

4) 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:

d. datę i godzinę zgłoszenia

e. opis Awarii lub Błędu

f. sposób naprawy oraz czas realizacji zlecenia.

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.

Załącznik nr 2a do Umowy nr…… z dnia…..

Protokół odbioru (wzór)

PROTOKÓŁ ODBIORU LICENCJI

UMOWA NR ……

Z DNIA ……

Data wykonania : …….

Data przeprowadzenia odbioru: …….

Miejsce przeprowadzenia odbioru: ……

Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …….

…….

…….

Przedstawiciele Wykonawcy: …….

…….

…….

Zgodność wykonania usługi z Umową:

Przekazanie dokumentów licencyjnych:……..

Wartość brutto oprogramowania/udzielanych licencji: ……zł (słownie…… zł)

Upoważniony przedstawiciel Wykonawcy: **Upoważniony przedstawiciel Zamawiającego:**

…… ……..

Załącznik nr 2b do Umowy nr.....z dnia…..

Protokół odbioru (wzór)
PROTOKÓŁ ODBIORU WDROŻENIA
UMOWA NR ……
Z DNIA ……

Data wykonania : …….
Data przeprowadzenia odbioru: …….
Miejsce przeprowadzenia odbioru: ……
Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …….
…….
…….
Przedstawiciele Wykonawcy: …….
…….
…….

Zgodność wykonania usługi z Umową:

Wykonanie wdrożenia (instalacji, konfiguracja, integracja oprogramowania: ……

Upoważniony przedstawiciel Wykonawcy: **Upoważniony przedstawiciel Zamawiającego**

…… ……..

Załącznik nr 2c do Umowy nrz dnia…..

Protokół odbioru (wzór)
PROTOKÓŁ PRZEPROWADZENIA INSTRUKTAŻU STANOWISKOWEGO
UMOWA NR ……
Z DNIA ……

Data wykonania : …….
Data przeprowadzenia odbioru: …….
Miejsce przeprowadzenia odbioru: ……
Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …….
…….
…….
Przedstawiciele Wykonawcy: …….
…….
…….
Zgodność wykonania usługi z Umową:

Przeprowadzenie instruktażu stanowiskowego dla administratorów zgodnie z §1 ust. 4: ……

Upoważniony przedstawiciel Wykonawcy: **Upoważniony przedstawiciel Zamawiającego:**

…… ……..

Załącznik nr 2d do Umowy nr.....z dnia…..

Protokół odbioru (wzór)
PROTOKÓŁ ODBIORU DOKUMENTACJI POWYKONAWCZEJ
UMOWA NR ……
Z DNIA ……

Data wykonania : …….
Data przeprowadzenia odbioru: …….
Miejsce przeprowadzenia odbioru: ……
Osoby dokonujące odbioru:

Przedstawiciele Zamawiającego: …….
…….
…….
Przedstawiciele Wykonawcy: …….
…….
…….

Zgodność wykonania usługi z Umową:

Wykonanie dokumentacji powykonawczej:
……

Upoważniony przedstawiciel Wykonawcy: **Upoważniony przedstawiciel Zamawiającego**

…… ……..

Załącznik nr 3 do Umowy nr. z dnia…..

Wzór oświadczenia o zachowaniu poufności

Ja niżej podpisany/a niniejszym oświadczam, że:

1) nie ujawnię bez stosownego upoważnienia wydanego przez Ministerstwo Sprawiedliwości, żadnych informacji, w szczególności prawnie chronionych, a także o sposobach zabezpieczenia stosowanych w Ministerstwie Sprawiedliwości, o ile wejdę w ich posiadanie, oraz nie przyczynię się do ich ujawnienia lub innych działań związanych z ich przetwarzaniem lub utratą itp. mogących spowodować szkodę dla Ministerstwa Sprawiedliwości, innych osób i podmiotów lub naruszenie przepisów prawa, w tym regulacji Ministerstwa Sprawiedliwości, zarówno w trakcie wykonywania prac w związku z zawartą przez ……umową …… jak i po ich zakończeniu oraz będę przestrzegał/a wszelkich przepisów w tym zakresie;
2) zobowiązuję się nie wykraczać poza nadane mi uprawnienia oraz zobowiązuję się wykorzystywać przydzielone mi środki pracy, w tym systemy i urządzenia informatyczne, tylko do celów realizacji ww. umowy;
3) zobowiązuję się przestrzegać oraz jestem świadomy/a odpowiedzialności za naruszenie obowiązujących zasad, wynikających w szczególności z:
   a) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
   b) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412),
   c) rozdziału XXXIII ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2017 r., poz. 2204 z późn. zm.).

_____	_____	_____
imię i nazwisko	PESEL	podpis

_____	_____
miejscowość	data

1. Dane osobowe zawarte w oświadczeniu są przetwarzane przez Ministra Sprawiedliwości z siedzibą w Warszawie, Al. Ujazdowskie 11 (00-950), który jest administratorem tych danych osobowych.
2. Dane osobowe zawarte w oświadczeniu są przetwarzane na podstawie art. 6 ust. 1 lit. b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

(ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05. 2016, str. 1).

3. Dane osobowe zawarte w oświadczeniu są przetwarzane w celu wykonania umowy oraz realizacji obowiązków Wykonawcy wynikających z umowy.
4. Dane osobowe zawarte w oświadczeniu nie będą przetwarzane w innym celu niż określony w pkt 3.
5. Dane osobowe zawarte w oświadczeniu nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowych.
6. Dane osobowe zawarte w oświadczeniu będą przechowywane przez okres 50 lat od dnia zakończenia realizacji umowy.
7. Ma Pan/Pani ma prawo żądać od administratora danych osobowych dostępu do danych osobowych zawartych w oświadczeniu, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, wniesienia sprzeciwu wobec przetwarzania i przenoszenia danych.
8. Odbiorcami danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
9. Przysługuje Panu/Pani prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych z siedzibą przy ul. Stawki 2, 00-193 Warszawa.
10. Dane osobowe zawarte w oświadczeniu nie będą podlegały profilowaniu (zautomatyzowanemu przetwarzaniu)
11. Podanie danych osobowych jest dobrowolne, jednakże odmowa ich podania uniemożliwi realizację przez Pana/Panią obowiązków wynikających z zawartej z Wykonawcą umowy.
12. W sprawach związanych z ochroną danych osobowych należy kontaktować się z Inspektorem Ochrony Danych (iod@ms.gov.pl).