Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest:

Przedmiotem zamówienia jest dostawa, uruchomienie, wdrożenie Oprogramowania do skanowania podatności infrastruktury Odbiorcy oraz świadczenie usług wsparcia technicznego na okres 36 miesięcy obejmującego:

- Monitorowanie podatności dla co najmniej 9595 hostów w różnych systemach operacyjnych.
- Monitorowanie podatności w środowiskach kontenerowych dla co najmniej 50 obrazów kontenerów.
- Monitorowanie podatności środowiska Web tj. dynamicznego testowania aplikacji webowych pozwalające na przeprowadzanie zautomatyzowanych testów penetracyjnych aplikacji webowych na minimum 50 adresów FQDN (Fully Qualified Domain Name) z możliwością rozszerzenia do 150 adresów bez ponoszenia dodatkowych kosztów związanych z licencją.
- Zarządzania zewnętrzną powierzchnią ataku dla co najmniej 3000 monitorowanych Hostów
- Przeprowadzenie instruktażu stanowiskowego dla wdrożonego Oprogramowania.

Odbiorca na potrzeby wdrożenia rozwiązania udostępni infrastrukturę niezbędną do uruchomienia maszyn wirtualnych. Wszystkie czynności związane z wdrożeniem i uruchomieniem Oprogramowania będzie wykonywał Wykonawca pod nadzorem Odbiorcy. Instalacja i aktualizacja Oprogramowania przez Wykonawcę odbywać się będzie w siedzibie Odbiorcy. Odbiorca może w drodze wyjątku wyrazić zgodę na wykonanie części prac zdalnie.

W ramach przedmiotu zamówienia stanowiącego **zamówienie** Wykonawca zobowiązuje się przenieść na Odbiorcę autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.

2. Wymagania dla przedmiotu zamówienia

I. Wymagania ogólne

1. Producent gwarantuje pokrycie co najmniej 90000 publicznie dostępnych CVE lub równoważny pod względem efektywności wykrywania podatności i zakresu pokrycia.
2. System dostarczony będzie w modelu w modelu „On- Premise”, z możliwością instalacji dodatkowych sensorów/appliance na infrastrukturze zamawiającego. Wymagane jest aby wyniki skanowania nie były przesyłane poza infrastrukturę Zamawiającego.
3. System jest zaprojektowany w architekturze klient-serwer.
4. Zarządzanie systemem, a w szczególności tworzenie raportów, danych analitycznych, kont użytkowników jest możliwe poprzez przeglądarkę internetową, bez instalacji dodatkowych konsoli lub komponentów.
5. Aktualizacje bazy podatności Systemu odbywają się co najmniej jeden raz dziennie (codzienna aktualizacja). System jest aktualizowany codziennie w sposób automatyczny. Ponadto

Oprogramowanie musi umożliwiać aktualizację zarówno silników skanowania jak i bazy podatności w trybie „z dostępem do sieci Internet" (automatycznie lub ręcznie), jak również w środowiskach odseparowanych od sieci Internet.

6. System zapewnia wsparcie dla uwierzytelniania z wykorzystaniem SAML lub MFA.
7. System ma możliwość tworzenia wielu użytkowników z różnymi poziomami uprawnień (RBAC).
8. System umożliwia eksport danych do formatów co najmniej CSV i PDF.
9. System ma możliwość eksportu raportów historycznych z co najmniej ostatnich 12 miesięcy.
10. System ma wbudowane możliwości integracji z narzędziami SIEM, ITSM oraz SOAR.
11. Komunikacja z System musi być szyfrowana protokołem HTTPS.
12. System ma możliwość rozbudowy platformy sprzętowej sensora.
13. System ma wbudowane możliwość automatyzacji procesów raportowania.
14. System ma wbudowane możliwość personalizacji alertów systemowych.
15. Wszystkie komponenty Systemu muszą pochodzić od jednego producenta.
16. Nie dopuszcza się rozwiązań typu open source.
17. Wszystkie komponenty systemu muszą być w pełni funkcjonalne i posiadać wsparcie producenta systemu przez okres trwania umowy tj. 36 miesięcy.
18. Wykonawca dostarczy samodzielną sondę do monitorowania podatności z funkcją dynamicznego testowania aplikacji webowych pozwalające na przeprowadzanie zautomatyzowanych testów penetracyjnych aplikacji webowych na minimum 5 adresów FQDN (Fully Qualified Domain Name)wraz z wszystkimi wymaganymi licencjami, oprogramowaniem dodatkowym.
19. System musi umożliwiać wdrożenie w pełnym on-premise w infrastrukturze bez dostępu do sieci Internet.
20. Rozwiązanie musi mieć możliwość wdrożenia jako:

- Aplikacja
- Urządzenie
- Maszyna wirtualna
- Rozwiązanie „chmurowe

21. Zwiększenie wydajności Systemu powinno być możliwe dzięki rozbudowaniu środowiska poprzez:

- Zmianę procesora
- Zwiększenie pamięci RAM
- Zwiększenie pojemności pamięci masowej
- Instalacji dodatkowych, nielimitowanych silników skanujących

22. Skanowanie podatności musi odbywać się na trzy sposoby:

- Skanowanie uwierzytelnione
- Skanowanie bez uwierzytelnienia
- Skanowanie przy użyciu agenta

II. Monitorowanie podatności hostów oraz środowisk kontenerowych musi posiadać co najmniej poniższe funkcjonalności

1. Skanowanie bez uwierzytelnienia.
2. Skanowanie uwierzytelnione komputerów, serwerów, stacji roboczych, serwerów do wirtualizacji (co najmniej VMware ESXi i vCenter), urządzeń sieciowych typu firewall, router, switch i baz danych oraz możliwość oceny ich pod kątem podatności rozumianych jako CVE oraz konfiguracji zgodnej z normami np. CIS lub wg najlepszych praktyk producenta.
3. Skanowanie agentowe dla co najmniej następujących systemów operacyjnych:

    - Kali Linux 2017 i wyższe,

- Debian 11 i wyższe,
- Fedora 40 i wyższe,
- Dystrybucje Linux typu RHEL 7 i wyższe (co najmniej AlmaLinux, Oracle Linux, Rocky Linux),
- Systemy dystrybucji komercyjnych (SUSE 12 SP5, SUSE Enterprise 15 SP2 i wyższe,
- macOS 13 i wyższe (Apple Silicon)
- Windows 10 i wyższe (w tym Windows 11)
- Windows Server od wersji 2012, do co najmniej wersji 2025.

4. Skanowanie pasywne z kopii ruchu.
5. Wsparcie integracji przez REST API.
6. Automatyczne aktualizacje skanerów.
7. Przechowywanie wyników skanowania centralnie.
8. Możliwość konfiguracji skanów według harmonogramów.
9. Automatyczne przypisanie ryzyka do hostów.
10. Możliwość edytowania przypisanych automatycznie wartości ryzyka.
11. Wykrywanie zmian podatności na hostach.
12. Wizualizacja historii podatności.
13. Możliwość raportowania według ustalonych harmonogramów.
14. Możliwość skanowania według standardów bezpieczeństwa (co najmniej CIS, DISA, Microsoft).
15. Panele zarządcze / dashboardy muszą być edytowalne. Tworzenie własnych dashboardów jest możliwe z biblioteki dostarczonej przez producenta. Musi istnieć możliwość tworzenia własnych raportów.
16. Eksport dashboardów/paneli zarządczych musi być możliwy do co najmniej PDF.
17. Wszystkie dane wyświetlane w panelach zarządczych muszą być automatycznie aktualizowane.
18. Do tworzenia własnych paneli zarządczych musi istnieć możliwość filtrowania danych i ich wyświetlania, co najmniej: krytyczność podatności (Critical, High, Medium, Low), wiek podatności, status uwierzytelnienia (Success, Insufficient Access, Authentication Failure), czas wykonania skanu, grupy zasobów, typy audytów.
19. Producent dostarcza wraz z rozwiązaniem panele zarządcze/dashboard'y które przedstawiają co najmniej: ogólny wgląd w zarządzanie podatnościami, analizę ryzyka dla assetów (kontekst biznesowy i podatności technicznych), raporty do zgodności ze standardami.
20. Dostęp do danych zarządzania podatnościami przez REST API.
21. Uwierzytelnianie API z wykorzystaniem kluczy.
22. Automatyczne wyzwalanie skanów podatności poprzez API.
23. Integracja z zewnętrznymi narzędziami analitycznymi w tym co najmniej SIEM.
24. Możliwość zarządzania dostępem do API.

III. Monitorowanie podatności środowiska Web tj. dynamicznego testowania aplikacji webowych DAST (Dynamic Application Security Testing) musi posiadać co najmniej funkcjonalności:

1. Tryby skanowania
   a. Pełne DAST: crawling, fuzzing, OWASP Top 10, injection, misconfig, exposure
   b. Rozróżnienie skanów aplikacji SPA i klasycznych stron HTML5
   c. Dedykowany tryb skanowania API: obsługa Swagger/OpenAPI/Postman
   d. Skanowanie aplikacji z formularzami logowania i sesją
   e. Weryfikacja poprawek przez re-scan delta
2. Integracje CI/CD

a. Pluginy i webhooki do Jenkins, GitHub Actions, GitLab CI/CD, Bamboo
b. Obsługa zmiennych środowiskowych w konfiguracjach skanów
c. REST API do zautomatyzowanego tworzenia, uruchamiania i pobierania wyników
d. Integracja z workflowem DevSecOps: ticketing, tagging, issue tracking

3. Autoryzacja i uwierzytelnienie
   a. Obsługa wielu metod auth: Basic, Form, OAuth2, SAML, certyfikaty, token JWT
   b. Selenium IDE do sesji logowania i sekwencji interakcji
   c. Maskowanie danych uwierzytelniających w logach i eksportach
4. Zarządzanie podatnościami
   a. Wykrywanie podatności w czasie rzeczywistym (strumieniowe API)
   b. Klasyfikacja wg OWASP, CVSS, CWE, CVE, własne kategorie
   c. Akceptacja, rekastowanie, przypisywanie priorytetów i właścicieli (asset-level)
5. Architektura
   a. Wsparcie dla skanów z Docker/OVA/Hyper-V
   b. Obsługa wielu lokalizacji: skanery lokalne i chmurowe
   c. Optymalizacja pod kątem latency, WAF, proxy, CSP
6. Zgodność
   a. Skanowanie zgodności z PCI DSS, SOC 2, ISO27001
   b. Możliwość filtrowania raportów do audytu wg kategorii
   c. Raportowanie trendów: regresje, SLA, czas reakcji na podatność

IV. Zarządzanie zewnętrzną powierzchnią ataku musi posiadać co najmniej funkcjonalności

1. System musi umożliwiać automatyczna identyfikacja zasobów internetowych na podstawie co najmniej nazwy domeny, adresu IP lub Autonomous System Number (ASN).
2. System musi umożliwiać automatyczne monitorowanie zmian w zasobach w ustalonych interwałach czasowych.
3. System musi umożliwiać monitorowanie na każdym ze znalezionych zasobów co najmniej:
   - Otwarte porty.
   - Uruchomione działające usługi
   - Bannery zwracane przez usługi działające na zasobach.
   - Szczegóły SSL/TLS (certyfikaty, daty ważności).
   - Nazwy serwerów DNS.
   - Adresy IP.
   - Dane geolokacyjne (kraj, miasto, szerokość i długość geograficzna).
   - Informacje o hosting providerze (w tym dostawca usług chmurowych).
   - Informacje o aplikacjach webowych (używane frameworki JavaScript, CMS, wtyczki WordPress).
   - Informacje dotyczące używanych baz danych oraz technologii programistycznych.
   - Dane dotyczące serwerów mailowych oraz proxy.
4. System musi posiadać integrację z platformą do monitorowania i oceniania podatności oraz umożliwiać automatyzację zadań.
5. System musi umożliwiać obsługę domen i subdomen.
6. System musi umożliwiać monitorowanie adresów IP.
7. System musi umożliwiać analizę konfiguracji SSL/TLS.
8. System musi umożliwiać monitorowanie certyfikatów i terminów ich ważności.
9. System musi umożliwiać integrację z narzędziami SIEM.
10. System musi umożliwiać powiadomienia o nowych zasobach.
11. System musi umożliwiać monitorowanie technologii używanych na stronach internetowych w tym szczegółowe informacje o wersji używanego oprogramowania opisywanej jako CPE.
12. Zarządzanie wyjątkami zasobów.

13. System musi umożliwiać Integracja z rozwiązaniami chmurowymi (co najmniej AWS, Azure).
14. System musi umożliwiać Automatyczne wykrywanie podatności zewnętrznych zasobów opisanych jako CVE.
15. System musi umożliwiać integracji z narzędziami ticketowania.
16. System musi umożliwiać integracji z narzędziami typu skaner podatności i skaner typu DAST.
17. System musi umożliwiać historyczne raportowanie stanu powierzchni ataku.
18. System musi umożliwiać tagowania zasobów.
19. System musi umożliwiać filtrowania danych w oparciu o co najmniej:
    - Filtracja według statusu certyfikatów SSL/TLS (ważność, data wygaśnięcia).
    - Filtrowanie według geolokalizacji (kontynent, kraj, miasto, strefa czasowa).
    - Filtrowanie według typu hostingu (np. hosting chmurowy).
    - Filtrowanie według typów usług (np. proxy, mail server, web server).
    - Filtracja według technologii używanych na stronie (np. JavaScript libraries, Web frameworks).
    - Filtracja według otwartych portów i aktywnych usług.
    - Filtracja według wartości CVSS oraz konkretnych CVE.
    - Filtrowanie według technologii używanych do zarządzania zasobami IT.
    - Filtracja według ekspozycji zasobu na internet (zasoby wewnętrzne/zewnętrzne).
    - Możliwość zaawansowanego filtrowania wielopoziomowego za pomocą operatorów logicznych AND/OR oraz nawiasów.
    - Filtracja według obecności określonych tagów.
20. System musi umożliwiać analizę szczegółów zasobów w oparciu o poziomy krytyczności.
21. System musi umożliwiać podział według rodzaju zagrożenia (np. SSL/TLS wygaśnięcie certyfikatu, otwarte porty).
22. System musi umożliwiać wizualizację szczegółów dotyczących sieci, usług, SSL/TLS, lokalizacji oraz szczegółowych danych HTTP.
23. System musi umożliwiać przypisywania statusu zasobów i aktualizacji informacji manualnie lub automatycznie.

V. Metody oceny ryzyka

System musi wspierać i dostarczać dane, które nadają priorytety przy technicznej i biznesowej analizie ryzyka cybernetycznego.

1. Ocena ryzyka w oparciu o dynamiczne dane dotyczące zagrożeń, które uwzględniają aktualne trendy zagrożeń, aktywność exploitów oraz publiczne informacje o podatnościach.
2. Analiza ryzyka na podstawie stopnia krytyczności zasobów, uwzględniająca wpływ na działalność biznesową organizacji.
3. Możliwość przypisania priorytetu do wykrytych podatności na podstawie prawdopodobieństwa wykorzystania podatności przez atakującego.
4. Wizualizacja ekspozycji ryzyka w postaci interaktywnych dashboardów.
5. Wsparcie dla oceny ryzyka na podstawie standardów branżowych, takich jak CVSS v2, CVSS v3 oraz innych standardów oceny podatności.
6. Automatyczne generowanie rekomendacji działań naprawczych w oparciu o identyfikowane ryzyko.
7. Wizualizacja trendów zmian poziomu ryzyka w czasie rzeczywistym oraz historycznie.
8. Możliwość tworzenia własnych kart oceny ryzyka opartych na kontekście biznesowym, np. jednostki biznesowe, lokalizacje fizyczne, systemy operacyjne.

9. Monitorowanie realizacji SLA napraw podatności w celu zapewnienia zgodności z wewnętrznymi politykami bezpieczeństwa.
10. Automatyczna analiza wpływu zdarzeń zewnętrznych na poziom ryzyka organizacji.
11. Automatyczne uwzględnienie podatności o wysokim poziomie ryzyka w raportach cyklicznych.
12. Analiza ekspozycji uwzględniająca różne klasy aktywów, np. aplikacje, infrastruktura IT, zasoby chmurowe.
13. Metoda kalkulacji ryzyka oparta na ocenie zagęszczenia podatności w odniesieniu do krytyczności zasobów.
14. Integracja wyników oceny ryzyka z zewnętrznymi platformami analitycznymi.
15. Automatyczne powiadamianie o przekroczeniu progów ryzyka ustalonych przez użytkownika.
16. Możliwość eksportu danych o ryzyku w formatach CSV, PDF, XML.
17. Zarządzanie wyjątkami w ocenie ryzyka dla specyficznych zasobów lub podatności.
18. Wizualizacja porównawcza poziomu ryzyka w odniesieniu do branżowych wskaźników.
19. Automatyczna klasyfikacja ryzyka zasobów zgodnie z predefiniowanymi kryteriami.
20. Integracja oceny ryzyka z narzędziami klasy SIEM, SOAR, ITSM oraz raportowanie wyników analizy ryzyka w narzędziach zewnętrznych.

3. Implementacja Oprogramowania

1. Wykonawca w terminie do 30 dni roboczych od daty podpisania umowy będzie odpowiedzialny za dostarczenie, instalację i konfigurację środowiska Oprogramowania w infrastrukturze Odbiorcy. 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 Odbiorcy w szczególności szczegółowy opis zakresu integracji Oprogramowania z infrastrukturą Odbiorcy.
   3) Opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Odbiorca, Wykonawca) niezbędnych do dostosowania Oprogramowania do potrzeb Odbiorcy i konfiguracji środowiska produkcyjnego.
   4) Szczegółowy opis koniecznych zmian w konfiguracji urządzeń sieciowych i serwerów Odbiorcy.
   5) Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu (zgodnie z postanowieniami Istotnych Postanowień Umowy) zawierający w szczególności: odbiór Dokumentacji Projektowej.
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 posiadanym przez Odbiorcę narzędziem Active Directory, serwerem DHCP, DNS,
4) Przeniesienie ustawień konfiguracyjnych z istniejącego środowiska Odbiorcy (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 zgodniej z formatem .doc lub .pdf.

4. Dokumentacja powykonawcza Oprogramowania

1. Wykonawca opracuje i dostarczy Odbiorcy w formie elektronicznej zgodnej z formatem .doc lub .pdf dokument „Dokumentacja powykonawcza" w terminie 15 dni roboczych.
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.

13) W terminie do 15 dni kalendarzowych od upływu okresu Gwarancji określonego w Umowie, Wykonawca przekaże Odbiorcy w formie plików archiwalnych wszelkie dane techniczne (logi, pliki robocze) związane z realizacją przedmiotowej Umowy, a następnie usunie wskazane dane techniczne z własnych zasobów. Przekazanie danych nastąpi na podstawie Protokołu Przekazania danych, którego wzór stanowi załącznik nr…… do Umowy.

14) W terminie do 30 dni kalendarzowych od upływu przekazania danych technicznych, o których mowa w pkt 13) Wykonawca przedłoży Odbiorcy Protokół Usunięcia danych, którego Wzór stanowi Załącznik nr …… do Umowy.

5. Instruktaż stanowiskowy dla wdrożonego Oprogramowania

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

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 Odbiorcy,
4. Zarządzanie wdrożonym Oprogramowaniem:
   a) możliwości rozbudowy, przyłączanie, 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 15 osób wskazanych przez Odbiorcę
   b) łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 2 dni robocze Odbiorcy.
   c) instruktaż stanowiskowy będzie prowadzony w siedzibie Odbiorcy lub innym miejscu wskazanym przez Wykonawcę i zaakceptowanym przez Odbiorcę

d) instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Oprogramowania,

e) instruktaż stanowiskowy powinien zostać przeprowadzony w dniach roboczych pracy Odbiorcy tj. pn – pt, w godzinach 8:30 – 15:30.

f) 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.

6. Warunki realizacji zamówienia i gwarancja dla Oprogramowania

1. Wykonawca udziela Odbiorcy 36 miesięcznej licencji na dostarczone w ramach umowy Oprogramowanie liczonej od daty podpisania protokołu odbioru przedmiotu zamówienia. W ramach udzielonej licencji Odbiorca 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 gwarantuje następujące czasy naprawy Oprogramowania, licząc od momentu zgłoszenia przez Odbiorcę:

   a) w ciągu 48 godzin w przypadku Awarii Oprogramowania (jako Awarię Odbiorca definiuje niedostępność Oprogramowania lub awarię Oprogramowania, która uniemożliwia jego wykorzystanie)

   b) w ciągu 72 godzin w przypadku Błędu w Oprogramowaniu (jako Błąd w Oprogramowaniu Odbiorca definiuje nieprawidłowe działanie Oprogramowania lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie Oprogramowania)

3. W ramach udzielonej Odbiorcy 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 Odbiorcy.

4. Wykonawca określi drogę dokonywania zgłoszeń serwisowych oraz przygotuje niezbędne dostępy pozwalające na dokonanie zgłoszenia przez pracowników Odbiorcy w terminie 15 dni roboczych od podpisania umowy. Wykonawca będzie prowadził całą historię złożonych zleceń oraz zapewni Odbiorcy wgląd do systemu zawierający opis wszystkich zgłoszeń w całym okresie realizacji umowy. Wykonawca zapewni Odbiorcy możliwość dokonywania zgłoszeń w trybie 24/7. Każde zgłoszenie złożone przez Odbiorcę powinno zawierać:
    a) datę i godzinę zgłoszenia
    b) opis Awarii lub Błędu
    c) sposób naprawy oraz czas realizacji zlecenia.

5. Odbiorca 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 Odbiorcę o zaistniałym fakcie.

7. Funkcjonalności Oprogramowania zgodnie z deklaracją w ofercie Wykonawcy podlegającą ocenie w ramach poza cenowych kryteriów oceny ofert:

W zależności od treści Oferty Wykonawcy podlegającej ocenie w ramach poza cenowych kryteriów oceny ofert Oprogramowanie będzie realizowało ponadto następujące funkcjonalności:

Funkcjonalność „zaawansowany suport" (F1):

☐ Oprogramowanie posiada zaawansowany support o parametrach nie mniejszych niż 24x7x365
P1-Critical: < 2 hr

P2-High: < 4 hr

P3-Medium: < 12 hr

P4-Informational: < 24 hr.

☐ nie posiada ww. funkcjonalności
** zaznaczyć właściwe*

Funkcjonalność „utworzenia specjalnego konta z uprawnieniami do tworzenia haseł dla skanów aktywnych" (F2)

☐ Oprogramowanie posiada możliwość utworzenia specjalnego konta z uprawnieniami do tworzenia haseł dla skanów aktywnych, a co za tym idzie odebrać możliwość tworzenia i podglądu haseł dla wszystkich innych kont stworzonych w Oprogramowaniu

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „natywna integracja z Jira" (F3)

☐ Oprogramowanie posiada natywną integrację z Jira

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „natywna integracja z systemem Manage engine Patch Manager Plus" (F4)

☐ Oprogramowanie posiada natywną integrację z systemem Manage engine Patch Manager Plus

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „on- premise" (F5)

☐ Oprogramowanie jest rozwiązaniem całkowicie „on-premise"

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „możliwość instalacji agentów rozwiązania na wybranych stacjach bez dodatkowych kosztów" (F6)

☐ Oprogramowanie posiada możliwość instalacji agentów rozwiązania na wybranych stacjach bez dodatkowych kosztów

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „możliwość przygotowania skanu czyszczącego pulę licencyjną z nie skanowanych adresów IP" (F7)

☐ Oprogramowanie posiada możliwość przygotowania skanu czyszczącego pulę licencyjną z nieskanowanych adresów IP

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*

Funkcjonalność „możliwość wykonywania skanu detekcyjnego dla nie ograniczonej ilości IP w sieci, bez uzależnienia od licencji produktu (tzw, discovery scan)" (F8)

☐ Oprogramowanie posiada możliwość wykonywania skanu detekcyjnego dla nie ograniczonej ilości IP w sieci, bez uzależnienia od licencji produktu (tzw, discovery scan)

☐ nie posiada ww. funkcjonalności

** zaznaczyć właściwe*