SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa, uruchomienie i wdrożenie systemu klasy Security Orchestration, Automation And Response (SOAR).

Zamawiający na potrzeby wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Wszystkie czynności związane z wdrożeniem Systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja Systemu przez Wykonawcę odbywać się będzie w siedzibie Zamawiającego. Zamawiający może wyrazić zgodę na wykonanie prac zdalnie w całości lub części

1. W ramach realizacji przedmiotu zamówienia mieści się:

1.1 Wdrożenie tj. dostawa, instalacja, konfiguracja i uruchomienie oferowanego Oprogramowania – zwanego dalej „Rozwiązaniem" , „Systemem" lub „Oprogramowaniem" w terminie do 30 dni roboczych od daty podpisania umowy.

1.2 Świadczenie serwisu i wsparcia technicznego Producenta elementów Rozwiązania przez okres obowiązywania umowy, licząc od daty podpisania bez uwag protokołu odbioru.

1.3 Gwarancja Producenta Rozwiązania świadczona przez okres obowiązywania umowy (18. 24 lub 36 miesięcy), licząc od daty podpisania bez uwag protokołu odbioru.

1.4 Przeprowadzenie instruktaży stanowiskowych dla 2 (dwóch) osób

1.5 Świadczenie serwisu i wsparcia technicznego Wykonawcy dla całego Rozwiązania przez okres obowiązywania umowy licząc od daty podpisania bez uwag protokołu odbioru.

1.6 Przeprowadzenie przez Wykonawcę wdrożenia oferowanego Rozwiązania.

1.7 Sporządzenie dokumentacji technicznej i powykonawczej.

2. Wymagania dotyczące dostawy sprzętu, oprogramowania oraz licencji:

2.1 Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca.

2.2 Całość dostarczanego Rozwiązania musi być nowa, wcześniej nieużywana.

2.3 Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, fabrycznie nowe, zakupione w autoryzowanym

kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski.

2.4 Dostarczane oprogramowanie na dzień złożenia oferty nie może być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia oprogramowania w EOL (brak wsparcia producenta lub wycofanie oprogramowania z oficjalnej dystrybucji).

2.5 Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików, na adres email wskazany przez Zamawiającego.

3. Wymagania dot. zakresu usług

3.1 System ma być dostarczony z licencją na wskazany przez Zamawiającego adres mailowy i objęty wsparciem technicznym Producenta przez okres wskazanym pkt 1.2 niniejszego SOPZ liczony od daty podpisania bez uwag protokołu odbioru wdrożenia Systemu.

3.2 W ramach wsparcia technicznego i gwarancji Producenta Zamawiający ma otrzymać:

a. bezpłatny dostęp do aktualizacji, poprawek i nowych wersji/kompilacji programu.
b. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez system zgłoszeniowy Producenta.
c. Gwarancja i serwis realizowany zdalnie, z czasem reakcji w zależności od poziomu krytyczności awarii/błędy od 1h do 12 godzin od przyjęcia zgłoszenia (szczegóły niżej), możliwość zgłaszania awarii poprzez dedykowany i zabezpieczony kanał komunikacji elektronicznej.
d. Gwarancja i serwis realizowany w trybie 24x7x365 1h Remote Response Time (w przypadku krytycznego poziomu błędu/awarii) oraz 24x7x365 do 8h w przypadku błędu niekrytycznego.
e. Szczegółowe warunki wsparcia technicznego dla Oprogramowania, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Oprogramowania, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności.
f. Dostęp do bazy wiedzy oraz dokumentacji Systemu.

3.3 Wymagania dot. wsparcia technicznego Wykonawcy Rozwiązania zostały określone w punkcie 5 niniejszego SOPZ

3.4 Wymagania dot. Projektu technicznego realizacji wdrożenia

a. Wykonawca przekaże Zamawiającemu Projekt techniczny, nie później niż 10 dni roboczych od dnia zawarcia Umowy,
b. Projekt techniczny realizacji wdrożenia dostarczonego Sprzętu i Oprogramowania, musi uwzględniać bezpieczeństwo Rozwiązania, dobre praktyki i rekomendacje eksploatacyjne publikowane przez Producenta dostarczonego oprogramowania. Zamawiający wymaga, aby projekt techniczny uwzględniał mechanizmy zapewniające wysoką dostępność (HA)
c. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia Projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub o konieczności wprowadzenia zmian, wszystkie uwagi do Projektu technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
d. Zamawiający w terminie do 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionego Projektu technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian,
e. komunikacja pomiędzy Zamawiającym, a Wykonawcą w zakresie zgłaszania uwag i akceptacji Projektu technicznego, odbywać się będzie drogą mailową na adresy poczty elektronicznej wskazane w Umowie,
f. zatwierdzony wspólny Projekt techniczny zostanie przekazany Zamawiającemu, w formie elektronicznej, na wskazany w umowie adres email, w postaci plików do edycji i PDF,

3.5 Wymagania dot. wdrożenia

Wykonawca będzie odpowiedzialny za dostarczenie, instalację, konfigurację oprogramowania i optymalizację środowiska Systemu w infrastrukturze Zamawiającego, a ponadto:

a. Zintegruje oprogramowanie z posiadanym przez Zamawiającego oprogramowaniem klasy SIEM – tj. Splunk Enterprise
b. Zintegruje oprogramowanie z posiadanymi przez Zamawiającego urządzeniami UTM i WAF tj. Fortigate, Palo Alto oraz F5 BigIP WAF.
c. Zintegruje oprogramowanie z posiadanym przez Zamawiającego oprogramowaniem zgłoszeniowym Atlassian Jira.
d. Zintegruje oprogramowanie z posiadanym przez Zamawiającego skanerem podatności Tenable Nessus.
e. Zintegruje oprogramowanie z posiadaną przez Zamawiającego usługą katalogową Microsoft Active Directory.

f. Przeprowadzi testy (niezawodnościowe oraz funkcjonalne) Rozwiązania oraz utworzy raporty z testów.
g. Opracuje Dokumentację powykonawczą na którą powinny się składać w informacje wymienione i opisane w pkt 3.7 niniejszego SOPZ.
h. Zapewni prawidłowe działanie Oprogramowania.
i. Przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w zakresie wskazanym w pkt 3.6 niniejszego SOPZ.

3.6 Wymagania dot. instruktaży stanowiskowych:

a. Instruktaże stanowiskowe będą prowadzone w języku polskim i obejmą zakresem m.in.:
    i. Użytkowanie Oprogramowania,
    ii. Budowę, architekturę i konfigurację Rozwiązania,
    iii. Administrowanie wdrożonym Rozwiązaniem;
b. Instruktaże stanowiskowe zostaną przeprowadzone przez przeszkolonych i certyfikowanych specjalistów danego Produktu.
c. Zamawiający dopuszcza przeprowadzenie instruktaży w trybie zdalnym.
d. Administratorzy Rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji Oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem Rozwiązania, a także sposoby przeciwdziałania im, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczone Oprogramowanie, jak również znać jego wdrożoną konfigurację.
e. Instruktarze stanowiskowe powinny się odbyć nie później niż 20 dni roboczych od daty podpisania bez uwag protokołu odbioru Rozwiązania.

3.7 Wymagania dot. dokumentacji powykonawczej

Dokumentacja powykonawcza powinna zawierać przynajmniej:

a. opis architektury technicznej tj. wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany),
b. wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu SOAR,

c. schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze,
d. przepływ danych w systemie (koncepcja obiegu informacji w Systemie pomiędzy poszczególnymi komponentami, warstwami Systemu,
e. szczegółową konfigurację poszczególnych elementów Systemu (np. serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www - zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji Systemu,
f. specyfikację i konfiguracja serwerów wirtualnych,
g. opis portów komunikacyjnych (opis powinien zawierać informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów,
h. rodzaje kont systemowych i ich uprawnienia (określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w systemie,
i. uprawnienia kont serwisowych,
j. role administracyjne,
k. ustawienia polityki haseł,
l. procedury zmiany haseł serwisowych, administracyjnych i użytkownika,
m. procedury weryfikacji uprawnień,
n. konfiguracja reguł firewall,
o. bezpieczeństwo transmisji (opis rozwiązań w zakresie zapewnienia poufności transmisji danych zarówno w sieci LAN/DMZ jak i Internet),
p. ochrona konfiguracji Systemu (ochrona krytycznych plików konfiguracyjnych),
q. opis rozwiązań w zakresie logowania zdarzeń (wskazanie rodzajów oraz lokalizacji dzienników w Systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury)
r. 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),
s. procedura odtwarzania Systemu (opisanie procedury backupu i odtworzenia całego Systemu i jego poszczególnych elementów, określenie czasu potrzebnego na odtworzenie całego Systemu oraz jego poszczególnych elementów, opis procedur przywracania Systemu do pełnej funkcjonalności po awarii),

t. procedura instalacji Systemu (opis procedury instalacji Systemu „od początku - krok po kroku", opis wszystkich kroków instalacji i konfiguracji Systemu w postaci zrzutów ekranu z opisami),
u. procedury wykonywania krytycznych operacji w Systemie (migracja, aktualizacja, itp.),
v. instrukcje obsługi Systemu dla Administratorów,
w. systemy zależne (np. agenci na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z Systemem, opis integracji z innymi usługami w tym w szczególności z MS Active Directory oraz MS Exchange.

4. Wymagania dot. oprogramowania

4.1. System musi zawierać mechanizm definiowania scenariuszy obsługi incydentów uruchamiany na podstawie następujących kryteriów:

4.1.1. w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe),

4.1.2. w przypadku gdy zasób jest elementem określonego procesu organizacji,

4.1.3. w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,

4.1.4. w przypadku, gdy na zasobie może dojść do określonego zagrożenia,

4.1.5. w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,

4.1.6. w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie

4.2. W ramach scenariuszy obsługi incydentów System musi umożliwić wykonanie następujących akcji i powiązanie ich z poszczególnymi krokami:

4.2.1. zmianę operatora,

4.2.2. zmianę statusu,

4.2.3. zmianę priorytetu,

4.2.4. przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API,

4.2.5. wysłanie powiadomień,

4.2.6. aktualizację dokumentów wraz z ich automatycznym wersjonowaniem,

4.2.7. gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu,

4.2.8. aktualizację list referencyjnych,

4.2.9. edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych,

4.2.10. założenie zadania.

4.3. System automatycznie musi proponować odpowiednie scenariusze obsługi incydentów. Scenariusze obsługi muszą zawierać możliwość ich symulacji i weryfikacji, m.in. na przykładowe zasoby IT.

4.4. Wymagana jest konfiguracja Systemu, w ramach której przebieg scenariusza dostosuje się dynamicznie do pozyskania w ramach jego obsługi informacji umożliwiając następujące funkcjonalności:

4.4.1. automatyzację wykonania wielu kroków nie wymagających reakcji operatora,

4.4.2. warunkowe wykonywanie kroków w zależności od informacji zawartej zarówno w elektronicznej dokumentacji, jak i informacji pozyskanej z innych systemów,

4.4.3. warunkowe wykonywanie kroków w zależności od odpowiedzi operatora na zdefiniowane pytanie.

4.5. System powinien posiadać gotowe integracje z producentami narzędzi do skanowania podatności (tzn. narzędzi Vunreability Assessment).

4.6. System na podstawie wyników skanowania podatności musi umożliwić identyfikowanie komputerów na podstawie ich nazw pozwalając tym samym na procesowanie podatności danego komputera przy dynamicznym adresie IP pobieranym z serwera DHCP.

4.7. System musi zawierać mechanizm definiowania scenariuszy obsługi podatności uruchamianych na podstawie następujących kryteriów:

4.7.1. w przypadku gdy na zasób przetwarza zdefiniowane informacje klasyfikowane, np. dane osobowe,

4.7.2. w przypadku gdy zasób jest elementem określonego procesu organizacji,

4.7.3. w przypadku gdy zasób zlokalizowany jest w danej lokalizacji,

4.7.4. w przypadku gdy na zasobie może dojść do określonego zagrożenia,

4.7.5. w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa,

4.7.6. w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie.

4.8. W ramach scenariuszy obsługi podatności System umożliwia:

4.8.1. zmianę operatora,

4.8.2. zmianę statusu,

4.8.3. zmianę priorytetu,

4.8.4. przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API.

4.8.5. wysłanie powiadomień.

4.8.6. aktualizację dokumentów wraz z ich automatycznym wersjonowaniem,

4.8.7. gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótu,

4.8.8. aktualizację list referencyjnych,

4.8.9. edycję bazy wiedzy zarówno w kontekście określonego wątku, jak i definiowania nowych,

4.8.10. założenie zadania.

4.9. System automatycznie musi proponować odpowiednie scenariusze obsługi podatności. Scenariusze obsługi muszą zawierać możliwości ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

4.10. System w razie wykrycia podatności o poważnych konsekwencjach dla organizacji musi umożliwić automatyczne powiadomienie o zdarzeniu wskazanych pracowników, m.in. email/sms.

4.11. System musi zapewnić możliwość tworzenia własnych wymagań bezpieczeństwa oraz ich weryfikacji względem zasobów IT, w tym serwerów, stacji roboczych oraz urządzeń sieciowych na bazie REST API, skryptów PowerShell/SSH.

4.12. System musi umożliwić rozbudowę list zgodności o wyniki działania przynajmniej jednego skanera podatności umożliwiającego przeprowadzenie skanowania typu COMPLIANCE (zgodność).

4.13. System musi umożliwić budowanie grupy wymagań dotyczących zgodności z normami czy rozporządzeniami pozwalając wpisać do Systemu poszczególne wymagania (np. punkty normy) oraz połączyć te wymagania ze skryptami je weryfikującymi. System pozwala na automatyczne zbudowanie raportu zgodności na podstawie wyników skryptów weryfikujących oraz innych parametrów elektronicznej dokumentacji.

4.14. System musi zawierać możliwość analizy poprawności konfiguracji poszczególnych elementów systemu teleinformatycznego np. przełączniki, systemu Firewall, serwery.

4.15. System musi realizować konfigurację schematu/ów klasyfikacji danych oraz schematu/ów klasyfikacji incydentów.Zaoferowany System musi umożliwiać skonfigurowanie przekierowania/skopiowania alarmów z narzędzia klasy SIEM.

4.16. Wykonawca zobowiązany jest do wykonania, w terminie 10 dni roboczych od podpisania umowy, logicznej architektury bezpieczeństwa teleinformatycznego Systemu. Architektura powinna opisywać urządzenia zabezpieczeń (Firewall, itp.), ich połączenia sieciowe oraz połączenia systemu bezpieczeństwa i adresy IP. oraz dodatkowo, w opracowanej architekturze należy uwzględnić systemy IT ważne dla organizacji (na podstawie danych przekazanych przez Zamawiającego), w ramach których możliwe do wystąpienia incydenty wymagają natychmiastowego działania.

4.17. Przygotowana przez Wykonawcę architektura bezpieczeństwa teleinformatycznego powinna być zaimplementowana w systemie IT oraz dodatkowo przekazana Zamawiającemu w postaci elektronicznej, tak, by mógł dokonać jej weryfikacji oraz dostrojenia scenariuszy obsługi incydentów i podatności bezpieczeństwa (tzn. wbudowanych playbooków) w ramach przyjętego procesu obsługi (tzn. Workflow). Zamawiający wymaga w ramach wdrożenia skonfigurowania maksymalnie do 20 playbooków. Playbooki muszą umożliwiać automatyzację pracy ludzi i integrację z zewnętrznymi źródłami danych, m.in. Threat Inteligence poprzez np. skrypty SSH/PowerShell, REST API lub inne.

4.18. Wymagane jest zapewnienie możliwości zweryfikowania działania wbudowanych w Systemie algorytmów szacowania ryzyka względem różnych wektorów ataków i w razie potrzeby dostrojenie parametrów dotyczących szacowania ryzyka.

4.19. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanych statystyk i raportów dotyczących obsługi incydentów i podatności bezpieczeństwa.

4.20. System musi umożliwiać generowanie raportów z obsługi incydentu w języku polskim.

4.21. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanej zawartości konsoli Dashboard i w razie potrzeby dostosowanie zakresu i sposobu prezentacji danych do potrzeb użytkownika.

4.22. Wymagane jest zapewnienie możliwości zweryfikowania predefiniowanych reguł priorytetyzacji incydentów bezpieczeństwa i w razie potrzeby ich dostrojenie.

4.23. Wymagane jest zapewnienie możliwości zweryfikowania wymagań SLA dla obsługi incydentów i podatności oraz zasad powiadamiania.

4.24. System musi zapewnić możliwość tworzenia własnych wymagań bezpieczeństwa oraz ich weryfikacji względem zasobów IT w tym (serwerów, stacji roboczych oraz urządzeń sieciowych), na bazie skryptów PowerShell/SSH oraz parametrów elektronicznej dokumentacji.

4.25. System musi pozwalać na automatyczne zbudowanie raportu zgodności na podstawie wyników skryptów weryfikujących stan faktyczny zasobów informatycznych oraz innych parametrów elektronicznej dokumentacji.

4.26. System musi umożliwiać rozbudowę raportu wymagań bezpieczeństwa poprzez dodanie nowych typów informacji i uwzględnienie ich w algorytmach oceny.

4.27. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem klasy SIEM – tj. Splunk Enterprise w zakresie pobierania i operowania na zdarzeniach.

4.28. Oprogramowanie musi posiadać możliwość integracji z urządzeniami UTM i WAF tj. Fortigate, Palo Alto oraz F5 BigIP WAF w zakresie co najmniej możliwości tworzenia i modyfikowania reguł bezpieczeństwa oraz blokowania aplikacji i adresów IP na tych urządzeniach.

4.29. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem zgłoszeniowym Atlassian Jira w zakresie zarządzania ticketami i akcjami na ticketach w tym systemie.

4.30. Oprogramowanie musi posiadać możliwość integracji z oprogramowaniem Tenable Nessus w zakresie obsługi podatności oraz tworzenia nowych skanerów podatności, pobierania raportów z tych skanów.

4.31. Oprogramowanie musi posiadać możliwość integracji z usługą katalogową Microsoft Active Directory, w zakresie modyfikowania obiektów znajdujących się w katalogu (np. wyłączanie konta użytkownika).

4.32. Oprogramowanie musi posiadać możliwość wyzwalania remediacji i akcji poprzez SSH, Powershell, CMD oraz REST.

5. Zakres wsparcia technicznego i serwisu Wykonawcy dla zakupionego Systemu:

5.1. Zakres serwisu i wsparcia technicznego Wykonawcy:

5.1.1. Zapewnienie systemu zgłoszeń, dostępnego dla upoważnionych pracowników Zamawiającego, w dni robocze (poniedziałek-piątek) od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy, spełniającego poniższe wymagania:

- system zgłoszeń musi obejmować następujące kanały zgłoszeń: serwis WWW, poczta elektroniczna, telefon,
- w ramach systemu zgłoszeń zapewnienie kanału WWW do śledzenia i aktualizacji zarejestrowanych zgłoszeń oraz zapewnienie możliwości automatycznego dodawania wpisów w systemie poprzez e-mail.

5.1.2. Usuwanie usterek i błędów z zachowaniem poniższych zasad:

- Usunięcie błędu krytycznego lub wykonanie obejścia błędu krytycznego (umożliwiającego korzystanie z Systemu) nastąpi w czasie 48h od przekazania zgłoszenia przez Zamawiającego. Jeżeli jednak bezpośrednią przyczyną powstania błędu krytycznego Systemu jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z Producentem Rozwiązania w terminie możliwie najszybszym z punktu widzenia Producenta, nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia.
- Usunięcie innych błędów nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- Usunięcie usterek nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- W przypadku braku możliwości usunięcia usterek i błędów w podanych wyżej terminach, Wykonawca niezwłocznie dostarczy i wdroży czasowo równoważne rozwiązanie zastępcze (workaround). Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego.
- Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni roboczych od daty jego wdrożenia.

5.1.3. Świadczenie wsparcia technicznego w zakresie funkcjonowania Systemu:

- Wymiar: 10 roboczogodzin miesięcznie, do wykorzystania przez cały okres trwania umowy. Zamawiający zastrzega sobie możliwość korzystania z usługi wsparcia technicznego w miarę identyfikowanych potrzeb, przez co możliwe jest nie wykorzystanie pełnej puli roboczogodzin. Minimalna liczba roboczogodzin jaką wykorzysta Zamawiający i za jaką zobowiązuje się wypłacić Wykonawcy wynagrodzenie wynosi 50% zamówionej puli, przez cały okres obowiązywania umowy;
- Dostępność: dni robocze od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy;
- Miejsce: zdalnie i na miejscu jeśli będzie to wymagane;
- Realizacja zadań wynikających z zakresu umowy;
- Wsparcie w pracach rozwojowych i zadaniach administracyjnych.

5.1.4. Wykonawca zapewni wsparcie techniczne przez okres obowiązywania umowy. Objęcie usługami wsparcia technicznego i serwisu musi zapewnić Zamawiającemu pełną gotowość Wykonawcy do świadczenia opisanych w

niniejszej specyfikacji usług od pierwszego dnia obowiązywania Umowy. Ponadto, świadczone usługi nie mogą negatywnie wpływać na uruchomione aplikacje biznesowe i inne systemy bezpieczeństwa informacji funkcjonujące u Zamawiającego.

5.1.5. Wsparcie techniczne musi być świadczone przez zespół składający się, z co najmniej dwóch inżynierów Wykonawcy, posiadających stosowne kompetencje, potwierdzone certyfikatem ukończenia szkolenia z technologii wdrożonego Rozwiązania.