*OPIS PRZEDMIOTU UMOWY – FORMULARZ CENOWY*

[Spis treści 1](#_Toc167095862)

[Administracja zdalna w chmurze 2](#_Toc167095863)

[Ochrona stacji roboczych 3](#_Toc167095864)

[Ochrona serwera 7](#_Toc167095865)

[Dodatkowe wymagania dla ochrony serwerów Windows 8](#_Toc167095866)

[Ochrona urządzeń mobilnych opartych o system Android 9](#_Toc167095867)

|  |
| --- |
| **WYMAGANIA DOTYCZĄCE SYSTEMU ANTYWIRUSOWEGO Z FIREWALL** |
| **Lp.** | Administracja zdalna w chmurze | **Spełnienie wymagańTAK/NIE\*** | **potwierdzenie spełniania wymagań** | **WARTOŚCI, PARAMETRY, DANE TECHNICZNE (wypełnia Wykonawca)** |
| 1 | Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. | TAK/NIE |  |   |
| 2 | Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. | TAK/NIE |  |   |
| 3 | Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL | TAK/NIE |  |   |
| 4 | Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. | TAK/NIE |  |   |
| 5 | Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. | TAK/NIE |  |   |
| 6 | Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. | TAK/NIE |  |   |
| 7 | Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. | TAK/NIE |  |   |
| 8 | Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. | TAK/NIE |  |   |
| 9 | Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. | TAK/NIE |  |   |
| 10 | Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. | TAK/NIE |  |  |
| 11 | Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. | TAK/NIE |  |  |
| 12 | Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. | TAK/NIE |  |  |
| **Lp.** | Ochrona stacji roboczych | **Spełnienie****wymagań****TAK/NIE\*** | **potwierdzenie spełniania wymagań** | **WARTOŚCI, PARAMETRY, DANE TECHNICZNE****(wypełnia Wykonawca)** |
| 1 | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). | TAK/NIE |  |  |
| 2 | Rozwiązanie musi wspierać architekturę ARM64. | TAK/NIE |  |  |
| 3 | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | TAK/NIE |  |  |
| 4 | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. | TAK/NIE |  |  |
| 5 | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | TAK/NIE |  |  |
| 6 | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | TAK/NIE |  |  |
| 7 | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | TAK/NIE |  |  |
| 8 | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. | TAK/NIE |  |  |
| 9 | Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. | TAK/NIE |  |  |
| 10 | Rozwiązanie musi integrować się z Intel Threat Detection Technology. | TAK/NIE |  |  |
| 11 | Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). | TAK/NIE |  |  |
| 12 | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | TAK/NIE |  |  |
| 13 | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | TAK/NIE |  |  |
| 14 | Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | TAK/NIE |  |  |
| 15 | Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. | TAK/NIE |  |  |
| 16 | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
 | TAK/NIE |  |  |
| 17 | Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. | TAK/NIE |  |  |
| 18 | Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. | TAK/NIE |  |  |
| 19 | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK/NIE |  |  |
| 20 | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). | TAK/NIE |  |  |
| 21 | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK/NIE |  |  |
| 22 | Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. | TAK/NIE |  |  |
| 23 | Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
 | TAK/NIE |  |  |
| 24 | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. | TAK/NIE |  |  |
| 25 | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. | TAK/NIE |  |  |
| 26 | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. | TAK/NIE |  |  |
| 27 | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. | TAK/NIE |  |  |
| 28 | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. | TAK/NIE |  |  |
| 29 | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. | TAK/NIE |  |  |
| 30 | W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. | TAK/NIE |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | Ochrona serwera | **Spełnienie****wymagań****TAK/NIE\*** | **potwierdzenie spełniania wymagań** | **WARTOŚCI, PARAMETRY, DANE TECHNICZNE****(wypełnia Wykonawca)** |
| 1 | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, UbuntuServer 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux EnterpriseServer (SLES) 15, Oracle Linux 8 oraz Amazon Linux. | TAK/NIE |  |  |
| 2 | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. | TAK/NIE |  |  |
| 3 | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | TAK/NIE |  |  |
| 4 | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. | TAK/NIE |  |  |
| 5 | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | TAK/NIE |  |  |
| 6 | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK/NIE |  |  |
| 7 | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | TAK/NIE |  |  |
| 8 | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. | TAK/NIE |  |  |
| **Lp.** | Dodatkowe wymagania dla ochrony serwerów Windows | **Spełnienie****wymagań****TAK/NIE\*** | **potwierdzenie spełniania wymagań** | **WARTOŚCI, PARAMETRY, DANE TECHNICZNE****(wypełnia Wykonawca)** |
| 1 | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. | TAK/NIE |  |  |
| 2 | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). | TAK/NIE |  |  |
| 3 | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. | TAK/NIE |  |  |
| 4 | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK/NIE |  |  |
| 5 | Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | TAK/NIE |  |  |
| 6 | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. | TAK/NIE |  |  |
| 7 | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. | TAK/NIE |  |  |
| 8 | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | TAK/NIE |  |  |
| 9 | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. | TAK/NIE |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Dodatkowe wymagania dla ochrony serwerów Linux** |  |  |  |
| 1 | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. | TAK/NIE |  |  |
| 2 | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. | TAK/NIE |  |  |
| 3 | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. | TAK/NIE |  |  |
| 4 | Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. | TAK/NIE |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | Ochrona urządzeń mobilnych opartych o system Android | **Spełnienie****wymagań****TAK/NIE\*** | **potwierdzenie spełniania wymagań** | **WARTOŚCI, PARAMETRY, DANE TECHNICZNE****(wypełnia Wykonawca)** |
| 1 | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. | TAK/NIE |  |  |
| 2 | Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. | TAK/NIE |  |  |
| 3 | Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). | TAK/NIE |  |  |
| 4 | Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. | TAK/NIE |  |  |
| 5 | Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:* usunięcie zawartości urządzenia,
* przywrócenie urządzenia do ustawień fabrycznych,
* zablokowania urządzenia,
* uruchomienie sygnału dźwiękowego,
* lokalizację GPS.
 | TAK/NIE |  |  |
| 6 | Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. | TAK/NIE |  |  |
| 7 | Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:* nazwę aplikacji,
* nazwę pakietu,
* kategorię sklepu Google Play,
* uprawnienia aplikacji,
* pochodzenie aplikacji z nieznanego źródła.
 | TAK/NIE |  |  |
|  |  |  |  |  |

## Przedmiotem zamówienia jest **zakup licencji oprogramowania ESET PROTECT Entry ON-PREM dla potrzeb Specjalistycznej Przychodni Lekarskiej dla Pracowników Wojska w Warszawie.**

## Okres ważności zakupionych licencji: od dnia …………… r. do dnia ……………. r. (oba rozumiane włącznie, czyli okres 36 miesięcy).

## Termin dostawy zamówienia: **5 (pięć) dni od dnia podpisania umowy**

## Zamawiający posiada obecnie licencję na oprogramowanie ESET PROTECT Essential ON-PREM – Antywirus (1 licencja na 180 urządzeń końcowych typu komputer, serwer), które obowiązują do dnia 12.11.2024 r.

## Rozszerzenie obecnie posiadanej licencji do wersji ESET PROTECT Entry ON-PREM (Antywirus + Firewall + Ochrona Serwerów) – 1 licencja na 240 urządzeń końcowych typu komputer, serwer na okres 36 miesięcy od dnia zawarcia umowy.

## Zamawiający wymaga, aby dostarczone oprogramowanie było dostępne w polskiej wersji językowej i działało na systemach operacyjnych Microsoft Windows 7/8/10/11 (32/64 bit), Windows Server 2016, Windows Server 2019, Windows Server 2022, Linux RHel.

## Zamawiający wymaga, aby zostały zachowane dotychczasowe nazwy użytkownika i hasła umieszczone na obecnym certyfikacie.

## Oprogramowanie i licencje muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

## Zamawiający wymaga dostarczenia certyfikatu potwierdzającego ważność dostarczonej licencji w formie papierowej oraz elektronicznej, gdzie musi zostać oznaczona ilość licencji, czas ich obowiązywania, klucz licencyjny, identyfikator publiczny, nazwę produktu oraz szczegółowy zakres zastosowania licencji (tj. stacje robocze, serwery, urządzenia mobilne, systemy wirtualne, hypervisory itp.)

## Licencjonowanie musi uwzględniać (w okresie obowiązywania gwarancji) prawo do bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych oraz wsparcie techniczne producenta lub autoryzowanego dystrybutora ww rozwiązania.

## Licencjonowanie musi uwzględniać prawo do najnowszej wersji zakupionego produktu przez cały okres obowiązywania gwarancji jak i prawo do instalacji wersji archiwalnych, zgodnych z systemami Windows 7 (32/64 bit) w trybie instalacji zdalnej (agent+instalacja wypychana).

## Licencjonowanie musi uwzględniać prawo do pobierania najnowszej bazy sygnatur wirusów przez cały okres obowiązywania ważności licencji.

## Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania.

## Powyższe wymagania odnoszą się do natywnej funkcjonalności oferowanego przedmiotu zamówienia, bez użycia dodatkowego oprogramowania.

## Producent zapewnia bezpłatne wsparcie techniczne w dniach roboczych tj. od poniedziałku do piątku, w godz. 8-16, drogą mailową (preferowana), lub telefoniczną z max SLA NBD.

## ***Ochrona poprzez dwuskładnikowe uwierzytelnianie***

## Wsparcie dla systemów z rodziny Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / WindowsServer 2019 Essentials.

## Rozwiązanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015/ 2016.

## Rozwiązanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016/2019.

## Rozwiązanie musi wspierać integrację z Microsoft Remote Desktop Web Access.

## Rozwiązanie musi wspierać integrację z Microsoft Terminal Services Web Access.

## Rozwiązanie musi integrację z Microsoft Remote Web Access.

## Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają technologię RADIUS.

## ***Aplikacja mobilna***

## Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.1 lub wyższej), iOS (9 lub wyższej), Windows Phone 8.1, Windows Mobile 10.

## Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.

## Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.

## Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.

## Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.

## Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego

## Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

|  |  |
| --- | --- |
| Cena jednostkowa netto: |  |
| Podatek VAT: |  |
| Cena jednostkowa brutto: |  |
| **Wartość netto 240 sztuk:** |  |
| **Podatek VAT:** |  |
| **Wartość brutto 240 sztuk:** |  |

## \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##  WYKONAWCA ZAMAWIAJĄCY