Załącznik Nr 1 do SWZ – Opis Przedmiotu zamówienia dla Części 1.

Część 1. Dostawa oprogramowania.

1. **Oprogramowanie typu SIEM o parametrach technicznych nie gorszych niż:**

Producent..... Nazwa..... **(wypełnia Wykonawca)**		
	Funkcje/ parametry	**Opis minimalnych wymagań**
Oprogramowanie typu SIEM	Minimalne funkcjonalności kluczowe	1. System do działania nie może wymagać agenta, 2. System musi być zainstalowany na systemie z rodziny Windows, 3. System musi pozwalać na podłączenie certyfikatu, w formacie .PFX oraz Java keystore, 4. System musi obsługiwać integracje z innymi systemami klasy SIEM, 5. Interfejs systemu oraz konfiguracji musi być w całości dostępny z poziomu przeglądarki internetowej (Microsoft EDGE, Mozilla Firefox, Google Chrome w aktualnych dostępnych wersjach), 6. System musi obsługiwać bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych, 7. System musi działać na pojedynczej bazie danych, 8. System musi posiadać wbudowane skrypty, które pozwalają na: a. backup bazy danych, b. odtworzenie bazy danych, c. zmianę bazy danych. 9. System może używać jednego konta do połączenia z domeną, 10. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji, 11. System musi umożliwiać zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego, 12. System musi umożliwiać audyt plików na serwerach, w określonym odstępie czasowym bez użycia agenta lub w czasie rzeczywistym przy użyciu agenta, 13. System musi posiadać wbudowane raporty dotyczące m.in.: a. wszystkich zmian plików i folderów, b. plikach zmodyfikowanych, c. plikach usuniętych, d. plikach przeniesionych, e. plikach utworzonych. 14. System musi umożliwiać analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie , a w szczególności: a. nietypową aktywność danego użytkownika, b. nietypową aktywność użytkownika na serwerze, c. nietypową ilość prób np. logowań, d. nietypowe godziny logowań użytkowników, e. nietypowe działania na plikach. 15. System musi posiadać gotowe raporty dla IBM iSeries (AS/400), 16. System musi posiadać wbudowany audyt zgodności NIST, 17. System musi posiadać wbudowany audyt zgodności PDPA, 18. System musi posiadać wbudowany audyt zgodności ISO 27001:2013, 19. System musi posiadać wbudowany audyt zgodności GDPR/RODO, 20. System musi posiadać wbudowane raporty dostosowane dla Windows event logów, 21. System musi posiadać funkcjonalność umożliwiającą wykorzystywanie logów Amazon Web Service (AWS) EC2 do wygenerowania czytelnych raportów, 22. System musi posiadać funkcjonalność umożliwiającą wysyłanie notyfikacji SMS oraz na e-mail, 23. System musi posiadać funkcjonalność umożliwiającą raportowanie i audytowanie Integralności plików,

		24. System musi posiadać funkcjonalność umożliwiającą raportowanie i audytowanie AD AZURE, 25. System musi posiadać funkcjonalność umożliwiającą wykonanie raportów kooperacyjnych, 26. System musi posiadać opcję umożliwiającą integracje z systemami do zarządzania incydentami, 27. System musi posiadać funkcjonalność umożliwiającą cykliczne importowanie plików logów, 28. System musi posiadać funkcjonalność umożliwiającą obsługę logów w postaci syslogów, 29. System musi umożliwiać importowanie i analizowanie plików zdarzeń, 30. System musi obsługiwać logi co najmniej z niżej wymienionych systemów operacyjnych: a. system Windows, b. system Linux, c. system Unix, d. wirtualizatory VMWare i Hyper-V. 31. System musi obsługiwać logi co najmniej z niżej wymienionych urządzeń: a. routery i przełączniki sieciowe (w tym Cisco, Hewlett-Packard i inne), b. urządzenia UTM (w tym Fortinet, Stormshield i inne), c. bazy danych Oracle, MySQL, MSSQL, d. serwery webowe, e. serwery DHCP, f. serwery FTP, g. inne źródła logów w formacie syslog. 32. System musi wspierać automatyczne wykrywanie hostów, 33. System musi umożliwiać konfigurowanie własnych widżetów i widoków, 34. System musi umożliwiać wyszukiwanie w logach za pomocą operatora logicznego, frazy, zakresów wartości, symboli wieloznacznych i wyszukiwania grupowego, 35. System musi umożliwiać filtrowanie zdarzeń przed zapisaniem ich w bazie danych, 36. System musi umożliwiać szyfrowanie plików archiwum logów, 37. System musi pozwalać na agregowanie i analizowanie informacje o bezpieczeństwie oraz umożliwiać zarządzanie zdarzeniami (SIEM), 38. System musi posiadać funkcjonalność umożliwiającą dodawanie własnych audytów zgodności, 39. System musi posiadać funkcjonalność umożliwiającą dodawanie niestandardowych raportów, 40. System musi posiadać funkcjonalność umożliwiającą alarmowanie w czasie rzeczywistym połączeń sieciowych z adresów IP widniejących na „czarnej liście”, 41. System musi posiadać uwierzytelnianie użytkowników zewnętrznych przez Active Directory i RADIUS Server , 42. System musi umożliwiać eksportowanie raportów w formatach CSV, PDF, 43. System musi umożliwiać wykonanie analizy trendów, 44. System musi umożliwiać wykonanie automatycznego polecenia lub akcji w przypadku alertów, 45. System musi posiadać moduł archiwizacji, przy jednoczesnej kompresji logów, co pozwala na oszczędność powierzchni dyskowej, 46. Licencjonowanie musi być oparte o liczbę hostów końcowych, z których zbierane będą informacje (ilość sztuk): a. serwerów Windows, b. serwerów plików Windows, c. stacji Roboczych, d. urządzeń opartych o syslog w tym urządzeń sieciowych, e. aplikacji, f. serwerów MS SQL, g. serwera IIS, h. serwerów Plików Linux. 47. System musi zawierać moduł sztucznej inteligencji i alarmowania o anomaliach,

		48. System nie może być licencjonowany na ilość zbieranych eventów, syslogów lub innych informacji, 49. System nie może być licencjonowany na ilość techników zalogowanych do systemu, 50. System musi posiadać możliwość integracji z systemami do badania podatności, 51. System musi posiadać silnik korelacji zdarzeń, 52. System musi posiadać funkcjonalność niestandardowego przeglądania i analizy logów, 53. System oprócz możliwości tworzenia własnej bazy raportowej, musi posiadać zestaw wbudowanych raportów dla różnego typu hostów,	
	Architektura Systemu	System instalowany jest na fizycznej lub wirtualnej maszynie użytkownika. System musi posiadać zintegrowaną, bezpłatną bazę danych.	
	Wymagania systemowe	**Procesor** (zalecany): minimum Intel 16 rdzeniowy 2.4 Ghz **Pamięć RAM** (zalecana) : minimum 52 GB, **Dysk** (zalecana): minimum 1.5 TB wolego miejsca, SSD **System operacyjny**: Windows Serwer 2016 lub nowszy.	
	Liczba obsługiwanych urządzeń	a. Serwerów Windows – min. 3 szt. b. Serwerów plików Windows – min. 1 szt. c. Stacji Roboczych – min. 400 szt. d. Urządzeń opartych o syslog w tym urządzeń sieciowych - min. 60 szt. e. Kontrolery domeny – min. 2 szt. f. Serwera IIS – min. 1 szt. g. Aplikacje – min. 13 szt. h. Serwer MSSQL – min. 3 szt. i. Moduł sztucznej inteligencji	**WYPEŁNIA WYKONAWCA:** a. Serwerów Windows – …….. szt. b. Serwerów plików Windows – …….. szt. c. Stacji Roboczych – …….. szt. d. Urządzeń opartych o syslog w tym urządzeń sieciowych - …….. szt. e. Kontrolery domeny – …….. szt. f. Serwera IIS – …….. szt. g. Aplikacje – …….. szt. h. Serwer MSSQL – …….. szt.
	Licencjonowanie	System musi posiadać licencję wieczystą producenta na system SIEM.	
	Wdrożenie	Dostawca zapewnia wdrożenie systemu.	
	Okres wsparcia oraz aktualizacji oprogramowania	Minimum 24 miesiące. Wsparcie musi być świadczone przez polski zespół techniczny, a także musi zawierać dostęp do bazy wiedzy o systemie.	
	Gwarancja i serwis	1. Usługi techniczne świadczone przez dostawcę muszą być objęte 24 miesięczna gwarancją. 2. W okresie obowiązywania gwarancji musi być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail, telefonicznie lub przez dedykowany do tego portal.	

2. Oprogramowanie do badania podatności na potencjalne zagrożenia o parametrach technicznych nie gorszych niż:

Producent..... Nazwa..... (wypełnia Wykonawca)		
Oprogramowanie do badania	**Funkcje/ parametry**	**Opis minimalnych wymagań**
	Minimalne funkcjonalności kluczowe	1. System musi umożliwiać jego instalację na systemie operacyjnym Windows i Windows Server, 2. Interfejs systemu oraz konfiguracji musi być w całości dostępny z poziomu przeglądarki internetowej (Microsoft EDGE, Mozilla Firefox, Google Chrome w aktualnych dostępnych wersjach) bez potrzeby instalacji dodatkowych komponentów na stacjach roboczych, 3. System musi posiadać wsparcie dla języka polskiego, 4. System musi posiadać architekturę agentową, 5. System musi umożliwiać instalację serwerów dystrybucyjnych w lokalizacjach zdalnych celem zbierania i wymiany informacji, 6. System musi wspierać minimum bazy danych takie jak: PostgreSQL 10.23 oraz MSSQL Server wersja 2008, 2012,2014,2016, 2018 i nowsze,

		7. System do działania nie może wymagać zakupienia dodatkowej licencji na serwer bazodanowy, 8. System musi umożliwiać dwustopniową autoryzację użytkownika, 9. System musi umożliwiać tworzenia statycznych i dynamicznych grup dla komputerów w wielu domenach, 10. System musi umożliwiać zarządzanie systemami operacyjnymi minimum: a. Linux: Ubuntu 10.04 i nowsze, b. Debian 7 i nowsze, c. Red Hat Enterprise Linux 8 i nowsze, d. CentOS 8 i nowsze, e. Fedora 19 i nowsze, f. Mandriva 2010 i nowsze, g. Linux Mint 13 i nowsze, h. OpenSuSE 11 i nowsze, i. SuSE Enterprise Linux 11 i nowsze j. Mac OS: 10.6 - Snow Leopard, k. 10.7 – Lion, l. 10.8 - Mountain Lion, m. 10.9 – Mavericks, n. 10.10 – Yosemite, o. 10.11 - EI Capitan, p. 10.12 – Sierra, q. 10.13 - High Sierra, r. 10.14 – Mojave, s. 11 Big Sur, t. 12 Monterey, u. Windows OS: od Vista i nowsze, v. Windows server 2003 i nowsze. 11. System musi rozpoznawać stacje robocze w ramach sieci Active Directory oraz grup roboczych, 12. System musi umożliwiać instalację i deinstalację aktualizacji aplikacji, 13. System musi posiadać możliwość aktualizacji zainstalowanych na stacjach roboczych i serwerach sterowników, 14. System musi posiadać możliwość aktualizacji BIOS dla komputerów marki Dell, 15. System musi posiadać funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, 16. System musi umożliwiać zarządzanie aplikacjami, minimum: a. Microsoft Office, b. Google Chrome, c. Opera, d. Skype, e. Mozilla Firefox, f. Adobe Reader, g. Adobe Acrobat, h. Java, i. 7zip. 17. System musi umożliwiać włączenie opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym, 18. System musi posiadać wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe, 19. Architektura systemu musi umożliwiać zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego, 20. System musi posiadać rozbudowany narzędzi zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menedżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami, 21. System musi umożliwiać dodanie nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory, 22. System musi umożliwiać generowanie następujących raportów:

		a. raporty dotyczące zagrożeń, b. raporty dotyczące wszystkich zdarzeń systemowych, c. raporty dotyczące zasobów zarządzanych. 23. System musi umożliwiać planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podane adresy mailowe, 24. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu, 25. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłane zapytania SQL do bazy danych z poziomu konsoli zarządzającej, 26. System musi posiadać funkcję zarządzania oceną podatności na zagrożenia, 27. System musi posiadać funkcję automatycznego skanowania zasobów z jednoczesnym wykrywaniem zasobów w domenie a także w grupie roboczej, 28. System musi posiadać możliwość wykrywania zagrożeń poprzez skanowanie zasobów objętych zarządzaniem, 29. System musi posiadać funkcję wykrywania luk systemowych takich jak: a. aplikacje zbliżające się do końca wsparcia, b. aplikacje typu peer to peer, c. aplikację wykorzystywane do udostępniania zdalnego pulpitu, d. zagrożeń typu Zero Day. 30. System musi posiadać funkcję wykrywania zagrożeń wynikających z: a. ataków na strony URL, b. ataków typu „Denial of Service”, c. ataków typu “ Brute force”, d. przejęcia sesji, e. clicjacking, f. ujawnienia kodu źródłowego. 31. System musi posiadać funkcję audytu portów TCP i UDP oraz uruchomionych na nich usługach, 32. System musi posiadać możliwość zdalnego zamykania systemu operacyjnego na komputerach z systemem Windows i Linux, 33. System musi posiadać moduł do zarządzania podatnościami na urządzeniach sieciowych w zakresie: a. poszukiwania luk w oprogramowaniu Firmware, b. naprawiania i zarządzania lukami w zabezpieczeniach, c. odnajdywania urządzeń sieciowych w organizacji, 34. System musi pozwalać na integrację z rozwiązaniami typu Help Desk.
	Architektura Systemu	System musi dawać możliwość instalacji na środowisku klienta i być zintegrowany z darmową bazą danych.
	Wymagania systemowe	**Procesor** (zalecany): minimum Intel Core i3 2.0 Ghz, 3MB cache (serwer fizyczny) minimum 4 wirtualne procesory 2.0 Ghz, 3 MB cache (maszyna wirtualna) **Pamięć RAM** (zalecana) : minimum 2 GB, **Dysk** (zalecana): minimum 10 GB wolego miejsca, **System operacyjny**: Windows Serwer 2016 lub nowszy.
	Liczba obsługiwanych urządzeń	a. Stacje robocze – min. 400 szt. b. Serwery Windows - min. 3 szt. c. Urządzenia sieciowe – min. 35szt. d. Technicy pracujący w systemie - min. 5 szt. **WYPEŁNIA WYKONAWCA:** a. Stacje robocze – …….. szt. b. Serwery Windows – …….. szt. c. Urządzenia sieciowe – …….. szt. d. Technicy pracujący w systemie – …….. szt.
	Licencjonowanie	System musi posiadać licencję wieczystą producenta na system do badania podatności.
	Wdrożenie	Dostawca zapewnia wdrożenie systemu.
	Okres wsparcia oraz aktualizacji oprogramowania	Minimum 24 miesiące. Wsparcie musi być świadczone przez polski zespół techniczny, a także musi zawierać dostęp do bazy wiedzy o systemie.
	Gwarancja i serwis	1. Usługi techniczne świadczone przez dostawcę mają być objęte 24 miesięczna gwarancją.

		2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail, telefonicznie lub przez dedykowany do tego portal.

3. Oprogramowanie do monitoringu Infrastruktury IT o parametrach technicznych nie gorszych niż:

Producent..... Nazwa..... (wypełnia Wykonawca)		
	Funkcje/ parametry	**Opis minimalnych wymagań**
Oprogramowanie do monitoringu Infrastruktury IT	Minimalne funkcjonalności kluczowe	1. System musi posiadać moduł automatycznych akcji pozwalający na wykonanie zestawu predefiniowanych działań rutynowych lub podczas awarii sieci, 2. System musi umożliwić obsługę sieci rozproszonych (Jednostek Organizacyjnych) poprzez np. instalację wieloserwerową na zasadzie serwer centralny i serwery pośredniczące oraz posiadać moduł do zarządzania konfiguracją aktywnych urządzeń sieciowych, 3. System musi umożliwiać ustawienie dynamicznych wartości progowych dla krytycznych monitorowanych parametrów, takich jak wydajność procesora, wykorzystanie pamięci oraz czas odpowiedzi, 4. System musi obsługiwać bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych, 5. System musi umożliwiać delegację uprawnień przynajmniej na dwa poziomy – administrator i użytkownik tylko do odczytu, 6. System musi umożliwiać zawężenie zakresu dostępu do określonych monitorowanych urządzeń, grup, modułów poszczególnemu użytkownikowi, 7. System musi pozwalać każdemu użytkownikowi na tworzenie własnych, dedykowanych pulpitów nawigacyjnych, 8. System musi zawierać osadzony moduł umożliwiający tworzenie zautomatyzowanych, wielopoziomowych procedur IT pozwalających na definiowanie ciągów weryfikacji, działań i reakcji na zdarzenia w sieci bez konieczności tworzenia skryptów i programowania, 9. System musi pozwalać na cykliczne (wg zdefiniowanego w systemie harmonogramu) skanowanie zdefiniowanych segmentów sieci w celu wykrywania nowych urządzeń i automatycznego rozpoznawania oraz dodawania ich do monitoringu, 10. System musi umożliwiać wykonanie automatycznych działań po wykryciu nowego urządzenia (np. przydzielenie do określonej grupy, dodanie określonych parametrów monitorowania, dodanie określonych profili powiadomień w oparciu o schemat nazwy DNS, adresu IP, kategorii lub typ urządzenia), 11. Konfiguracje urządzeń sieciowych pozyskiwane przez system muszą być przechowywane w bazie danych systemu a nie w formie plików natywnych zarządzanych urządzeń, 12. Dane konfiguracji odczytane z urządzeń muszą być przechowywane w bazie w formie zaszyfrowanej, 13. System musi umożliwiać oznaczenie zarchiwizowanych wersji konfiguracji urządzeń jako konfiguracji bazowej, aktualnie funkcjonującej lub roboczej, 14. System musi umożliwiać przeglądanie danych z czujników sprzętowych związanych z macierzami dyskowymi i systemami taśmowymi, 15. System musi umożliwiać wysyłanie powiadomień i alertów, również na komunikatory takie jak, np. Teams, 16. System musi obsługiwać monitorowanie WLC, 17. System musi obsługiwać monitorowanie sprzętu oparte na IPMI, 18. System musi umożliwiać monitorowanie Meraki REST API, 19. System musi posiadać funkcję „SDN monitoring for Cisco Application Centric Infrastructure (ACI)" pozwalającą monitorować sieć szkieletową, grupy punktów końcowych oraz ogólną wydajność środowiska Cisco ACI, 20. System musi pozwalać na integrację z systemami typu Help Desk,

		21. System musi pozwalać zbiorczo aktualizować protokoły monitorowania dostępności (ICMP, TCP, i SNMP). 22. System musi umożliwiać planowanie i eksportowanie zintegrowanych raportów w formacie pliku XLS, 23. System musi umożliwiać monitorowanie stanu dysku, portu, wentylatora, zasilania, baterii, wartości czujnika temperatury dla urządzeń NetApp ONTAP (CLUSTER), 24. System musi umożliwiać monitorowanie stanu i kondycji dysku modeli urządzeń z serii IBM DS, 25. System musi umożliwiać użytkownikowi włączanie lub wyłączanie dodatkowych modułów, 26. System musi umożliwiać nadanie użytkownikowi uprawnień do odpowiednich modułów zgodnie z posiadanymi uprawnieniami, 27. System musi umożliwiać tworzenie profili indywidualnych dla użytkownika, 28. System musi umożliwiać monitorowanie VPN (Site-to-Site) przez następujących dostawców: Cisco, Watchguard, Fortinet, Barracuda, ZyXEL, Stormshield, Checkpoint, Juniper, Palo Alto itp., 29. System musi umożliwiać działanie agentowe w przypadku kiedy serwer straci połączenie z siecią, w tym czasie agent musi gromadzić dane a po przywróceniu łączności niezwłocznie przesłać je do serwera głównego. System musi posiadać do komunikacji agent – serwer „Push Mode”, 30. System musi pozwalać na dodawanie przez użytkowników znaków w notatkach o alarmach, 31. System musi umożliwiać włączenie uwierzytelniania dwuskładnikowego (TFA), dla administratorów systemu, 32. System musi posiadać wsparcie dla języka polskiego,
	Architektura Systemu	1. System musi posiadać funkcję monitoringu infrastruktury IT dla monitorowania i obrazowania stanu urządzeń sieciowych, 2. System musi posiadać możliwość rozszerzenia funkcjonalności o dodatkowe moduły np.: a. moduł analizy wysycenia pasma w technologii Flow, b. moduł do zarządzania konfiguracją aktywnych urządzeń sieciowych, c. modułu zarządzania adresacją IP oraz portami przełączników sieciowych, d. moduł analizy logów zapór sieciowych, 3. Wszystkie moduły systemu muszą być dostępne z poziomu jednej konsoli użytkownika bez konieczności przełączania się między odrębnymi systemami i bez konieczności instalacji dodatkowych wtyczek, 4. System musi umożliwiać aktywowanie i dezaktywowanie poszczególnych modułów bez potrzeby ingerencji w pliki systemowe, 5. Architektura systemu musi umożliwiać instalację serwerów dystrybucyjnych w lokalizacjach zdalnych, umożliwiając zarządzanie urządzeniami końcowymi bez konieczności łączenia się z serwerem głównym i nadmiernego obciążania łącza, 6. System musi posiadać zwiększony zakres bezpieczeństwa polegający na obowiązkowej konfiguracji weryfikacji dwuskładnikowej podczas uwierzytelniania logowania do panelu aplikacji, 7. System do działania nie może wymagać zakupienia dodatkowej licencji na serwer bazodanowy, 8. System musi posiadać bazę danych PostgreSQL w wersji min 10.20 lub nowszą, 9. System musi posiadać bibliotekę JFreeChart jar w wersji min 0.9.19 lub nowszą, 10. System musi posiadać bibliotekę JCommon jar w wersji min. 0.9.4 lub nowszą, 11. System musi posiadać jQuery w wersji min. 3.6.0 lub nowszą, 12. System musi posiadać jQuery UI w wersji min. 1.13.1 lub nowszą, 13. System musi posiadać zwiększone bezpieczeństwo podczas aktualizacji aplikacji poprzez konieczność zaimportowania certyfikatu w trakcie dokonywania podniesienia wersji, 14. System musi obsługiwać uwierzytelnianie oparte na SAML 2.0.

	Wymagania systemowe	1. Wszystkie składniki systemu muszą pochodzić od jednego producenta, 2. System musi działać zarówno w środowisku Windows Server w wersji co najmniej 2016 (wersje zarówno 32 jaki 64 bit) jak i w 64bitowym środowisku Linux, 3. Wszystkie elementy muszą wpierać działanie w środowisku wirtualnym opartym na Vmware, 4. System musi wspierać bazy danych PostgreSQL oraz MSSQL, 5. System musi obsłużyć sieć rozproszoną umożliwiając instalację wieloserwerową na zasadzie serwer centralny i serwery pośredniczące, 6. Interfejs oprogramowania oraz konfiguracji musi być dostępny w całości z poziomu przeglądarki internetowej (Microsoft EDGE, Mozilla Firefox ,Google Chrome w aktualnych wersjach) bez potrzeby instalacji dodatkowych komponentów na stacjach roboczych. **Procesor** (zalecany): minimum Intel Xeon 3.5 Ghz (serwer fizyczny) minimum 8 wirtualne procesory 3.5 Ghz, (maszyna wirtualna) **Pamięć RAM** (zalecana) : minimum 16 GB, **Dysk** (zalecana): minimum 100 GB wolego miejsca, **System operacyjny**: Windows Serwer 2016 lub nowszy.	
	Liczba obsługiwanych urządzeń	a. Urządzenia – min. 40 urządzeń (SNMP, WMI, Telnet/SSH) b. Administratorzy systemu – min. 5 szt	**WYPEŁNIA WYKONAWCA:** a. Urządzenia – urządzeń (SNMP, WMI, Telnet/SSH) **–** …….. urządzeń. b. Administratorzy systemu **–** …….. szt.
	Licencjonowanie	System musi posiadać licencję wieczystą producenta na system do monitorowania infrastruktury IT.	
	Wdrożenie	Dostawca zapewnia wdrożenie systemu.	
	Okres wsparcia oraz aktualizacji oprogramowania	Minimum 24 miesiące. Wsparcie musi być świadczone przez polski zespół techniczny, a także musi zawierać dostęp do bazy wiedzy o systemie.	
	Gwarancja i serwis	1. Usługi techniczne świadczone przez dostawcę mają być objęte 24 miesięczna gwarancją. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail, telefonicznie lub przez dedykowany do tego portal.	