Nr sprawy: .....
Załącznik nr 1 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia:

Przedmiotem zamówienia jest rozbudowa i modernizacja infrastruktury bezpieczeństwa teleinformatycznego Zamawiającego poprzez usługę rozszerzenia funkcjonalności posiadanych systemów bezpieczeństwa, dostawę urządzeń oraz dostawę systemu klasy Deception.

II. Zakres przedmiotowego zamówienia obejmuje 3 zakresy o charakterystyce opisanej poniżej:

Struktura bezpieczeństwa i centralnego zarządzania infrastrukturą informatyczną Zamawiającego, oparta jest na rozwianiach marki Fortinet.
Zamawiający w najbliższej przyszłości nie planuje zmiany rozwiązań w powyższym zakresie z uwagi na zbyt wysokie koszty związane ze zmianą ww. infrastruktury, wdrożeniem i szkoleniem zasobów ludzkich w poruszaniu się w nowej technologii. Wprowadzenie rozwiązań innego producenta powodowałoby konieczność migracji środowiska, rekonfiguracji systemów oraz generowałoby istotne ryzyko operacyjne i dodatkowe koszty, co jest nieuzasadnione z punktu widzenia ciągłości działania oraz bezpieczeństwa Zamawiającego oraz jego ekonomicznego interesu.

Celem zapewnienia zachowania spójności technologicznej z eksploatowaną infrastrukturą teleinformatyczną oraz kompatybilności z funkcjonującymi systemami bezpieczeństwa i centralnego zarządzania, Zamawiający wymaga dostawy rozwiązań kompatybilnych z posiadaną infrastrukturą:

A. Usługa rozszerzenie funkcjonalności dla:

1) ***Urządzeń FortiGate 600E (s/n:*** **FG6H0ETB20900406, FG6H0ETB20900363**).

   Rozszerzenie funkcjonalności o:
   a) *Attack Surface Security Rating*
   b) *Operational Technology (OT) Security Service*

Zamawiający wymaga, aby okres dostępności wszystkich posiadanych oraz rozszerzonych funkcjonalności był zgodny z okresem obowiązywania wsparcia technicznego tak aby pozostawały one aktywne co najmniej do dnia ***15.07.2027 r****.*

2) ***Systemu FortiWeb (s/n: FVVM04TM21001070):***

   Rozszerzenie funkcjonalności o:
   a) Advanced Bot Protection
   b) Client-Side Protection

Zamawiający wymaga, aby okres dostępności wszystkich posiadanych oraz rozszerzonych funkcjonalności był zgodny z okresem obowiązywania wsparcia technicznego tak aby pozostawały one aktywne co najmniej do dnia ***06.12.2027 r****.*

3) Systemu FortiAnalyzer (s/n: FAZ-VMTM26011731):

Rozszerzenie funkcjonalności o:

a) OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules(for 1- 101 GB/Day of Logs)
b) Outbreak Detection Service
c) SOAR Security Automation Service
d) Security Rating Update

*Zamawiający wymaga, aby okres dostępności wszystkich posiadanych oraz rozszerzonych funkcjonalności był zgodny z okresem obowiązywania wsparcia technicznego tak aby pozostawały one aktywne co najmniej do dnia **02.06.2027 r**.*

Sposób realizacji:

1. Zamówienie zostanie uznane za zrealizowane, po sprawdzeniu przez Zamawiającego statusu danej funkcjonalności w aspekcie jej poprawnego działania/aktywacji.

2. W ramach realizacji zamówienia Wykonawca zapewni udostępnienie wszystkich funkcjonalności wskazanych w niniejszym OPZ dla posiadanego przez Zamawiającego urządzenia lub systemu.

   Zamawiający musi zachować co najmniej dotychczasowy zakres funkcjonalny oraz uzyskać funkcjonalności wymagane w niniejszym OPZ.

B. Dostawa urządzeń UTM (typ I oraz typ II) wraz z zapewnieniem wsparcia technicznego producenta oraz niezbędnymi funkcjonalnościami na okres 12 miesięcy:

Struktura bezpieczeństwa i centralnego zarządzania infrastrukturą informatyczną Zamawiającego, oparta jest na rozwianiach marki Fortinet.
Zamawiający w najbliższej przyszłości nie planuje zmiany rozwiązań w powyższym zakresie z uwagi na zbyt wysokie koszty związane ze zmianą ww. infrastruktury, wdrożeniem i szkoleniem zasobów ludzkich w poruszaniu się w nowej technologii. Wprowadzenie rozwiązań innego producenta powodowałoby konieczność migracji środowiska, rekonfiguracji systemów oraz generowałoby istotne ryzyko operacyjne i dodatkowe koszty, co jest nieuzasadnione z punktu widzenia ciągłości działania oraz bezpieczeństwa Zamawiającego oraz jego ekonomicznego interesu.

Celem zapewnienia zachowania spójności technologicznej z eksploatowaną infrastrukturą teleinformatyczną oraz kompatybilności z funkcjonującymi systemami bezpieczeństwa i centralnego zarządzania, Zamawiający wymaga dostawy urządzeń kompatybilnych z posiadaną infrastrukturą o parametrach nie gorszych niż:

Urządzenia TYP I - Tabela parametrów technicznych – wymagania minimalne: (2 szt.).

Lp.	Parametr	Wymaganie minimalne Zamawiającego
1. Specyfikacja sprzętowa		
1	Porty WAN	Minimum 2 × sprzętowo akcelerowane porty GE WAN
2	Porty LAN RJ45	Minimum 6 × sprzętowo akcelerowane porty GE RJ45
3	Porty FortiLink	Minimum 2 × sprzętowo akcelerowane porty GE RJ45 FortiLink (domyślnie)
4	Porty PoE	Brak wymagań – urządzenie nie musi posiadać portów PoE
5	Port USB	Minimum 1 × port USB
6	Port konsoli	Minimum 1 × port konsolowy RJ45

7	Pamięć wewnętrzna	Brak wymagań – urządzenie nie musi posiadać wbudowanej pamięci wewnętrznej
8	Trusted Platform Module	Urządzenie musi posiadać moduł TPM
9	Bluetooth	Wbudowany moduł Bluetooth Low Energy (BLE)
10	Bezpieczeństwo firmware	Obsługa podpisanego firmware oraz sprzętowy przełącznik zabezpieczeń
11	Porty antenowe	Minimum 3 × port antenowy (SMA)
12	Łączność bezprzewodowa	Urządzenie musi posiadać wbudowany interfejs bezprzewodowy Dual Radio (2,4 GHz / 5 GHz) zgodny ze standardami 802.11 a/b/g/n/ac/ax (Wi-Fi 6 lub nowszy).
2. Wydajność systemowa – Enterprise Traffic Mix		
13	Przepustowość IPS	Minimum 2,5 Gb/s
14	Przepustowość NGFW	Minimum 1,5 Gb/s
15	Przepustowość Threat Protection	Minimum 1,3 Gb/s
3. Wydajność i pojemność systemu		
16	Firewall Throughput	Minimum 10 Gb/s (dla pakietów 1518 / 512 / 64 byte UDP)
17	Opóźnienie zapory	Maksymalnie 2,46 µs (dla pakietów UDP 64 byte)
18	Przepustowość pakietowa	Minimum 15 Mpps
19	Sesje równoczesne	Minimum 1,4 mln sesji TCP
20	Nowe sesje	Minimum 100 000 sesji TCP/s
21	Polityki firewall	Minimum 5000
22	IPsec VPN Throughput	Minimum 7,1 Gb/s (pakiety 512 byte)
23	Tunele IPsec Gateway-to-Gateway	Minimum 200
24	Tunele IPsec Client-to-Gateway	Minimum 500
25	SSL Inspection Throughput	Minimum 1,4 Gb/s
26	SSL Inspection CPS	Minimum 715
27	SSL Inspection Concurrent Sessions	Minimum 140 000
28	Application Control Throughput	Minimum 3,6 Gb/s
29	CAPWAP Throughput	Minimum 6,8 Gb/s
30	Virtual Domains (VDOM)	Minimum 10 (domyślnie i maksymalnie)
31	Obsługa FortiSwitch	Minimum 24 przełączniki
32	Obsługa FortiAP	Minimum 96 punktów dostępowych (w tym min. 48 w trybie tunelowym)
33	FortiTokens	Minimum 500
34	Wysoka dostępność	Obsługa trybów Active-Active, Active-Passive oraz Clustering

4. Generacja urządzenia	
35	Oferowane urządzenie musi pochodzić z aktualnej, najnowszej linii produktowej producenta dostępnej na dzień składania ofert, nie może być przeznaczone do wycofania (End of Sale) ani znajdować się w statusie End of Support. Zamawiający wymaga dostawy urządzenia z najnowszej generacji sprzętowej producenta.
5. Funkcjonalności / mechanizmy bezpieczeństwa	
1	Wraz z urządzeniem Wykonawca zobowiązany jest zapewnić, na okres nie krótszy niż **12 miesięcy**, pełny dostęp do usług, funkcjonalności oraz wsparcia producenta, niezbędnych do korzystania co najmniej z następujących funkcji bezpieczeństwa: a) systemu zapobiegania włamaniom IPS wraz z bieżącą aktualizacją sygnatur; b) ochrony antywirusowej i antymalware wraz z bieżącą aktualizacją sygnatur; c) kontroli aplikacji; d) filtrowania adresów URL i kategoryzacji stron internetowych; e) filtrowania zapytań i domen DNS; f) filtrowania treści wideo; g) wykrywania i blokowania komunikacji z sieciami botnet oraz serwerami Command and Control; h) analizy podejrzanych plików w środowisku sandbox producenta, świadczonym jako usługa chmurowa; i) ochrony antyspamowej; j) dostępu do aktualizacji systemu operacyjnego urządzenia;

1. **Wsparcie techniczne producenta** – musi być dostępne na zasadach przewidzianych dla minimum poziomu FortiCare Premium Support., dostępnych na stronie Producenta pod adresem: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forti-care-services.pdf
2. **Aktualizacje i poprawki** – możliwość pobierania i instalacji najnowszych wersji oraz poprawek bezpieczeństwa dostarczanych przez producenta.
3. **Dostęp do dokumentacji i bazy wiedzy** – zapewnienie dostępu do oficjalnej dokumentacji oraz zasobów producenta.
4. **Możliwość pobierania aktualizacji** – dostęp do wszystkich aktualizacji oprogramowania za pośrednictwem strony internetowej producenta.
5. **Dostęp do portalu zgłoszeń** – możliwość zgłaszania incydentów i problemów technicznych poprzez oficjalny portal wsparcia producenta.
6. **Okres wsparcia technicznego producenta** – 12 miesięcy.

Urządzenia TYP II - Tabela parametrów technicznych – wymagania minimalne: (2 szt.).

Lp.	Parametr	Wymaganie minimalne Zamawiającego
1. Specyfikacja sprzętowa		
1	Porty WAN Combo	2 x sprzętowo akcelerowane porty WAN 10GE SFP/SFP+ oraz 2,5/5/10GE RJ45
2	Porty LAN RJ45	Minimum 8 × sprzętowo akcelerowane porty GE RJ45 10/100/1000Mbps
3	Port USB	1 × port USB
4	Port konsoli	1 × port konsolowy RJ45
5	Pamięć wewnętrzna	Brak wymagań – urządzenie nie musi posiadać wbudowanej pamięci wewnętrznej

6	Trusted Platform Module	Urządzenie musi posiadać moduł TPM
7	Bluetooth	Wbudowany moduł Bluetooth Low Energy (BLE)
8	Montaż	Wersja desktopowa
2. Wydajność systemowa – Enterprise Traffic Mix		
1	Przepustowość IPS	Minimum 4,5 Gb/s
2	Przepustowość NGFW	Minimum 2,5 Gb/s
3	Przepustowość ochrony przez zagrożeniami	Minimum 2,2 Gb/s
3. Wydajność i pojemność systemu		
1	Przepustowość zapory sieciowej (firewall)	Minimum 27,9 Gb/s (dla pakietów 1518 / 512 / 64 byte UDP)
2	Opóźnienie zapory (firewall)	Maksymalnie 3,25 µs (dla pakietów UDP 64 byte)
3	Przepustowość pakietowa	Minimum 41,85 Mpps
4	Sesje równoczesne	Minimum 3 mln sesji TCP
5	Nowe sesje	Minimum 124 000 sesji TCP/s
6	Polityki firewall	Minimum 5000
7	Przepustowość tunelu IPsec	Minimum 25 Gb/s (pakiety 512 byte)
8	Tunele IPsec Gateway-to-Gateway	Minimum 200
9	Tunele IPsec Client-to-Gateway	Minimum 2500
10	Przepustowość inspekcji SSL	Minimum 2,5 Gb/s
11	Inspekcja SSL	Minimum 1400 nowych połączeń/sek.
12	Ilość konkurencyjnych sesji inspekcji SSL	Minimum 300 000
13	Przepustowość kontroli aplikacji	Minimum 6,7 Gb/s
14	Przepustowość CAPWAP	Minimum 23,6 Gb/s
15	Ilość wirtualnych instancji urządzenia możliwych do wygenerowania	Minimum 10 (domyślnie i maksymalnie)
16	Ilość przełączników możliwa do zarządzania z urządzenia	Minimum 24 przełączniki
17	Ilość accesspointów możliwa do zarządzania z urządzenia	Minimum 96 punktów dostępowych (w tym min. 48 w trybie tunelowym)
18	Ilość tokenów producenta urządzenia możliwa do zarządzania z urządzenia	Minimum 500
19	Wysoka dostępność (HA)	Obsługa trybów Active-Active, Active-Passive oraz Clustering

4. Generacja urządzenia	
1	Oferowane urządzenie musi pochodzić z aktualnej, najnowszej linii produktowej producenta dostępnej na dzień składania ofert, nie może być przeznaczone do wycofania (End of Sale) ani znajdować się w statusie End of Support. Zamawiający wymaga dostawy urządzenia z najnowszej generacji sprzętowej producenta.
5. Funkcjonalności / mechanizmy bezpieczeństwa	
1	Wraz z urządzeniem Wykonawca zobowiązany jest zapewnić, na okres nie krótszy niż **12 miesięcy**, pełny dostęp do usług, funkcjonalności oraz wsparcia producenta, niezbędnych do korzystania co najmniej z następujących funkcji bezpieczeństwa: a) systemu zapobiegania włamaniom IPS wraz z bieżącą aktualizacją sygnatur; b) ochrony antywirusowej i antymalware wraz z bieżącą aktualizacją sygnatur; c) kontroli aplikacji; d) filtrowania adresów URL i kategoryzacji stron internetowych; e) filtrowania zapytań i domen DNS; f) filtrowania treści wideo; g) wykrywania i blokowania komunikacji z sieciami botnet oraz serwerami Command and Control; h) analizy podejrzanych plików w środowisku sandbox producenta, świadczonym jako usługa chmurowa; i) ochrony antyspamowej; j) dostępu do aktualizacji systemu operacyjnego urządzenia;

1. **Wsparcie techniczne producenta –** musi być dostępne na zasadach przewidzianych dla minimum poziomu FortiCare Premium Support, dostępnych na stronie Producenta pod adresem: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf
2. **Aktualizacje i poprawki** – możliwość pobierania i instalacji najnowszych wersji oraz poprawek bezpieczeństwa dostarczanych przez producenta.
3. **Dostęp do dokumentacji i bazy wiedzy** – zapewnienie dostępu do oficjalnej dokumentacji oraz zasobów producenta.
4. **Możliwość pobierania aktualizacji** – dostęp do wszystkich aktualizacji oprogramowania za pośrednictwem strony internetowej producenta.
5. **Dostęp do portalu zgłoszeń** – możliwość zgłaszania incydentów i problemów technicznych poprzez oficjalny portal wsparcia producenta.
6. **Okres wsparcia technicznego producenta** – 12 miesięcy

C. Dostawa systemu wykrywania zagrożeń wewnętrznych klasy Deception (systemu pułapek i przynęt sieciowych) w wersji wirtualnej, wraz ze wsparciem technicznym producenta na okres minimum 12 miesięcy*:*

Przedmiotem zamówienia jest dostawa systemu wykrywania zagrożeń wewnętrznych klasy Deception (systemu pułapek i przynęt sieciowych) w wersji wirtualnej (jako maszyna wirtualna), wraz ze wsparciem technicznym producenta na okres minimum 12 miesięcy.

Opis obecnego środowiska systemowego Zamawiającego
Nowo wdrażany system klasy Deception musi charakteryzować się pełną, natywną i bezproblemową integracją z posiadaną przez Zamawiającego infrastrukturą bezpieczeństwa IT. Zamawiający posiada środowisko złożone z następujących systemów firmy Fortinet: FortiGate, FortiAnalyzer, FortiWeb, FortiSandbox, FortiMail, FortiEMS oraz FortiAuthenticator, które działają w zintegrowanym środowisku Fortinet Security Fabric.

Oferowane rozwiązanie musi w pełni i natywnie współpracować z wyżej wymienionymi komponentami, umożliwiając m.in. automatyczną wymianę danych telemetrycznych o zagrożeniach oraz automatyczną izolację zagrożeń.

1. **Wymagania techniczne (środowisko wirtualizacji)**

Kompatybilność z hypervisorem:
System musi być dostarczony w formacie umożliwiającym bezpośrednie uruchomienie i stabilną pracę na platformie wirtualizacyjnej VMware vSphere ESXi (wersja 7.0 lub nowsza).

Alokacja zasobów:
Zamawiający zapewnia zasoby wirtualne w ramach własnej infrastruktury sprzętowej.
Minimalne dopuszczalne parametry alokacji zasobów dla maszyny wirtualnej muszą wynosić:

a) Procesory: minimum 4 vCPU (lub więcej, zależnie od liczby uruchamianych maszyn-przynęt).
b) Pamięć operacyjna: minimum 8 GB RAM (z zachowaniem rekomendacji dynamicznego przydziału dodatkowej pamięci RAM na każdą instancję maszyny-przynęty - Decoy VM).
c) Przestrzeń dyskowa: wsparcie dla dysków wirtualnych o pojemności od 200 GB do 16 TB.
d) Wirtualne interfejsy sieciowe: obsługa do 6 wirtualnych kart sieciowych (vNIC).

2. **Szczegółowe wymagania funkcjonalne:**

Oferowany system wirtualny musi spełniać następujące wymagania funkcjonalne i operacyjne:

1. Integracja z ekosystemem Fortinet Security Fabric: Rozwiązanie musi natywnie współdzielić dane o wykrytych zagrożeniach z systemami FortiGate, FortiAnalyzer oraz FortiSandbox. System musi automatycznie generować i przekazywać reguły blokowania (Inline Quarantine) do firewalli FortiGate w celu natychmiastowego odcięcia atakującego hosta od sieci.

2. Obsługa i monitorowanie sieci VLAN: System musi posiadać zdolność do jednoczesnego działania, nasłuchiwania ruchu i aktywnego rozproszenia przynęt w oparciu o co najmniej 4 odrębne sieci wirtualne (VLAN) przy wykorzystaniu interfejsów typu trunk (standard 802.1Q).

3. Skalowalność przynęt i adresacji IP: Pojedyncza instancja systemu wdrożona na platformie VMware musi zapewniać równoległą obsługę do 20 wirtualnych maszyn-przynęt (Decoy VMs)

4. Zróżnicowanie systemów operacyjnych przynęt (Decoys): Możliwość jednoczesnego uruchamiania i utrzymywania w strukturze sieciowej fałszywych zasobów opartych o systemy operacyjne klasy Windows, Ubuntu/Linux, macOS, a także systemy dedykowane dla środowisk IoT oraz systemy automatyki przemysłowej i SCADA.

5. Wielowarstwowa architektura Deception: System musi wspierać symulację środowisk na trzech poziomach interakcji:
   a) Przynęty serwerowe i końcowe.
   b) Przynęty średniej interakcji (Medium interaction decoys dla urządzeń sieciowych, IoT i OT).
   c) Przynęty wysokiej interakcji (High interaction decoys) w pełni emulujące realne systemy operacyjne i aplikacje biznesowe.

6. Generowanie tokenów i śladów (Deception Tokens/Lures): Narzędzie musi pozwalać na masowe generowanie i dystrybucję tzw. "okruchów chleba" (breadcrumbs) oraz fałszywych poświadczeń (np. tokeny aplikacyjne, mapowania dysków sieciowych, zapamiętane hasła w przeglądarkach) instalowanych na realnych stacjach roboczych i serwerach, w celu przekierowania uwagi intruza na maszyny pułapki.

7. Ochrona Proaktywna i Analiza TTP: System musi natychmiastowo wykrywać działania z zakresu rekonesansu sieciowego, kradzieży tożsamości, ataków typu ransomware oraz prób utrzymania stałego dostępu. Każdy incydent musi być poddawany automatycznej analizie taktyk, technik i procedur (TTP) i korelowany z bazą wiedzy MITRE ATT&CK.

8. Centralna konsola zarządzania i logowanie: Dostęp do zarządzania systemem (konfiguracja, wdrażanie przynęt, alertowanie i analityka) musi odbywać się z poziomu dedykowanego panelu GUI. Wszystkie alerty i logi systemowe muszą być przesyłane natywnie do systemu FortiAnalyzer w celu konsolidacji zdarzeń.

3. Gwarancja i wsparcie techniczne producenta:

1. Wykonawca zobowiązany jest do dostarczenia wraz z rozwiązaniem oficjalnego wsparcia technicznego producenta.

2. Wsparcie techniczne producenta musi być dostępne przez co najmniej 8 godzin dziennie, 5 dni w tygodniu, w trybie nie gorszym niż 8×5.

3. Wsparcie musi gwarantować dostęp do wszelkich poprawek bezpieczeństwa, aktualizacji oprogramowania oraz baz sygnatur, silników analitycznych i subskrypcji ochrony dla oferowanego systemu.

4. Czas trwania usługi: minimum 12 miesięcy.

4. Wdrożenie:

Wykonawca przeprowadzi kompleksowe wdrożenie systemu klasy Deception w środowisku Zamawiającego, obejmujące co najmniej instalację, konfigurację, uruchomienie oraz integrację z posiadanymi przez Zamawiającego systemami teleinformatycznymi i bezpieczeństwa.

W ramach wdrożenia Wykonawca:

a) przeprowadzi analizę środowiska Zamawiającego oraz uzgodni szczegółową architekturę i sposób wdrożenia systemu;
b) zainstaluje i skonfiguruje wszystkie wymagane komponenty systemu;
c) skonfiguruje elementy pozorujące, profile, polityki detekcji, mechanizmy alarmowania oraz konta i uprawnienia administratorów;
d) przeprowadzi integrację systemu z usługami katalogowymi, systemami monitorowania, systemem klasy SIEM oraz innymi wskazanymi przez Zamawiającego rozwiązaniami;
e) dostosuje konfigurację systemu do specyfiki infrastruktury i wymagań bezpieczeństwa Zamawiającego;
f) przeprowadzi testy poprawności działania, w tym testy generowania, przekazywania i obsługi alertów;
g) usunie błędy i nieprawidłowości stwierdzone podczas testów;

h) przekaże Zamawiającemu dokumentację powdrożeniową, obejmującą co najmniej opis architektury, konfiguracji, integracji, kont administracyjnych, procedur eksploatacyjnych oraz wykonywania kopii zapasowych konfiguracji.

5. Warsztaty:

Wykonawca przeprowadzi warsztaty powdrożeniowe dla administratorów systemu klasy Deception.

Warsztaty zostaną zrealizowane w języku polskim, w formie praktycznej, z wykorzystaniem wdrożonego środowiska.

Zakres warsztatów obejmie co najmniej: omówienie architektury i konfiguracji systemu, bieżącą administrację, monitorowanie zdarzeń i alertów, analizę wykrytych incydentów, zarządzanie elementami pozorującymi, integrację z pozostałymi systemami bezpieczeństwa, wykonywanie kopii konfiguracji oraz podstawowe czynności diagnostyczne.

- Czas trwania warsztatów: co najmniej 10 godzin, podzielonych na min. 2 spotkania;
- Zajęcia muszą być przeprowadzone w języku polskim;
- Warsztaty mogą się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00 lub stacjonarnej w siedzibie Zamawiającego;
- Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim lub angielskim;
- Liczba uczestników: 6;

III. Wymagania dotyczące realizacji:

1. Usługi muszą być świadczone zgodnie z zasadami określonymi przez producenta urządzeń i systemów posiadanych przez Zamawiającego, określonych powyżej.

2. Zamawiający musi mieć zapewniony dostęp do portalu zgłoszeń producenta oraz możliwość pobierania wszystkich dostępnych aktualizacji oprogramowania.

3. Realizacja zamówienia nie może powodować przerwy w dostępie do dotychczas posiadanych usług, funkcjonalności, aktualizacji oprogramowania ani wsparcia technicznego.

4. Wszystkie usługi, uprawnienia oraz funkcjonalności objęte zamówieniem muszą zostać przypisane bezpośrednio do urządzeń, systemów oraz konta Zamawiającego w systemie producenta.