

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu prowadzonym w trybie otwartej procedury konkurencyjnej pn.
**„Wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa
dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o.,
w ramach projektu „Cyberbezpieczne Wodociągi”**

CZĘŚĆ III – Dostawa oprogramowania SIEM wraz z usługą chmurową i wdrożeniem

Przedmiotem zamówienia jest dostawa, wdrożenie i uruchomienie systemu klasy SIEM wraz z usługą chmurową, konfiguracją, szkoleniem oraz wsparciem technicznym.

Przedmiot zamówienia

1. Przedmiotem Zamówienia jest kompleksowa usługa w zakresie dostawy, wdrożenia, konfiguracji, uruchomienia i utrzymania systemu do monitoringu infrastruktury teleinformatycznej i sieciowej Zamawiającego wraz z usługami towarzyszącymi, na którą składają się:
 - a) realizacja kompleksowego zadania polegającego na dostarczeniu infrastruktury teleinformatycznej IaaS (chmury obliczeniowej) wraz z oprogramowaniem i usługą chmurową.
2. Realizacja przedmiotu zamówienia, o którym mowa w ust. 1 pkt. a powyżej musi zostać przygotowana technologicznie w sposób umożliwiający zwiększanie ilości poszczególnych komponentów środowiska teleinformatycznego IaaS bez wpływu na ciągłość działania całego środowiska teleinformatycznego IaaS dostarczanego w ramach przedmiotu Zamówienia, tzn. bez wykonywania przerwy w działaniu i dostępie do środowiska IaaS w związku z jego rozbudową lub zwiększeniem.

Szczegółowy zakres prac

Dostarczenie infrastruktury teleinformatycznej IaaS na potrzeby systemu Bezpieczeństwa SIEM wraz z konfiguracją.

Wykonawca zobowiązany jest dostarczyć infrastrukturę teleinformatyczną w modelu usługowym chmury obliczeniowej IaaS dla systemu SIEM, w tym:

- a) zapewnić dostępność HA wszystkich dostarczonych zasobów IaaS na czas trwania Umowy;
 - 1) skonfigurować i utrzymywać dostarczone instancje serwerowe (VM);
 - 2) instalować, utrzymywać i aktualizować na instancjach serwerowych (VM) systemy operacyjne (Linux);
 - 3) skonfigurować i utrzymywać wewnętrzne połączenia sieciowe pomiędzy poszczególnymi instancjami serwerowymi oraz pozostałymi komponentami;
 - 4) skonfigurować i udostępnić łącza do sieci Internet, zgodnie z określonymi w OPZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować operacje i zadania instancji serwerowych oraz pozostałych komponentów

- zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę;
- 5) skonfigurować i utrzymywać ochronę na styku z Internetem w warstwie sieciowej;
 - 6) świadczyć usługę administrowania uruchomionymi instancjami serwerowymi (VM) do poziomu systemu operacyjnego;
 - 7) zapewnić niezbędne licencje i oprogramowanie związane z realizacją przedmiotu zamówienia.
- b) Zamawiający oczekuje dostarczenia infrastruktury teleinformatycznej w modelu usługowym chmury obliczeniowej IaaS z lokalizacji PDC, spełniającej minimalne wymogi bezpieczeństwa opisane w OPZ.
 - c) Zamawiający oczekuje zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres obowiązywania Umowy.
 - d) Zamawiający oczekuje udostępnienia stałego w trybie 24/7/365 dostępu do dedykowanego panelu klienta, w celu bezpośredniego monitorowania i weryfikowania dostarczonych parametrów IaaS.
 - e) Zamawiający oczekuje wdrożenia i skonfigurowania systemu SIEM w dostarczonej infrastrukturze IaaS na potrzeby zbierania i przechowania logów zdarzeń z urządzeń sieciowych Zamawiającego w celu stałego monitorowania wydajności rozwiązania i na wezwanie Zamawiającego każdorazowo udostępnić informacje w tym zakresie.
 - f) Zamawiający oczekuje uruchomienia infrastruktury teleinformatycznej w modelu chmury obliczeniowej IaaS o parametrach pozwalających na prawidłowe działanie dostarczonego systemu SIEM oraz archiwizacji logów zdarzeń nie krócej niż do 31.12.2026.
 - g) Zamawiający oczekuje uruchomienia dodatkowej infrastruktury teleinformatycznej w modelu chmury obliczeniowej o parametrach:
 - 1) Przestrzeń dyskowa na potrzeby kopii zapasowej systemów Zamawiającego 1 TB
 - 2) Zasoby IaaS o parametrach 8 vCPU / 16 GB RAM / 1TB GB SSD
 - 3) Usługę kopii zapasowej dla 3 maszyn wirtualnych wraz z oprogramowaniem
 - h) Zamawiający oczekuje, że do zadań realizowanych przez Wykonawcę w ramach dostarczonej infrastruktury IaaS należeć będzie administracja zasobami informatycznymi Wykonawcy w zakresie:
 - 1) utrzymania i aktualizacji całego środowiska IaaS,
 - 2) instalacji i konfiguracji systemów operacyjnych,
 - 3) instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska HA,
 - 4) aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
 - 5) utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
 - 6) realizacji bieżących czynności administracyjnych,
 - 7) utrzymania i aktualizacji zainstalowanego systemu SIEM
 - 8) przyjmowania zgłoszeń technicznych,
 - 9) analiz incydentów oraz problemów wraz z pełnym przywracaniem funkcjonalności.

Wymagania funkcjonalne dla systemu SIEM:

- a) Dostarczenie rozwiązania klasy SIEM dla dostarczonej infrastruktury teleinformatycznej w warstwie sprzętowej (m.in.: macierze, serwery, przełączniki

sieciowe) oraz warstwie oprogramowania na niej zainstalowanego (m.in. systemy operacyjne, aplikacje, bazy danych, etc.), spełniające poniższe wymagania:

- 1) system SIEM musi zapewniać skalowalną architekturę spełniającą następujące wymagania;
- 2) system SIEM musi umożliwiać gromadzenie, korelację zdarzeń przesyłanych lub pobieranych z innych systemów;
- 3) monitorowanie zdarzeń bezpieczeństwa;
- 4) analiza logów i detekcja anomalii;
- 5) kompatybilność z istniejącą infrastrukturą IT;
- 6) możliwość łatwego rozszerzenia funkcjonalności w przyszłości;
- 7) zapewnienie wsparcia z obowiązującymi regulacjami takimi jak: PCI DSS, HIPAA, NIST 800-53, TSC, GDPR;
- 8) możliwość zbierania logów z różnych źródeł;
- 9) analiza zachowań i detekcja anomalii;
- 10) predefiniowany zestaw reguł detekcji;
- 11) możliwość generowania alertów na podstawie wykrytych zagrożeń;
- 12) możliwość skonfigurowania automatycznych reakcji automatycznych na określone zdarzenia;
- 13) integracja z systemami zgłoszeniowymi (ticketowymi);
- 14) odpowiednie zabezpieczenia dostępu do systemu;
- 15) intuicyjny interfejs do konfiguracji i zarządzania systemem;
- 16) możliwość łatwej aktualizacji i rozbudowy systemu;
- 17) oprogramowanie SIEM zostanie dostosowane na potrzeby zbierania informacji i informowania o incydentach z systemów oraz urządzeń;
- 18) system SIEM będzie wspierać integrację z różnymi systemami i narzędziami, w tym serwerami, firewallami, systemami IDS, systemami NAC, systemami kontroli dostępu, systemami zarządzania tożsamością w tym Active Directory;
- 19) SIEM będzie obsługiwać różne protokoły transmisji logów, takie jak Syslog, SNMP, WMI i inne;
- 20) SIEM umożliwi zbieranie, normalizację i korelację logów z różnych źródeł w jednolitym formacie;
- 21) system musi umożliwiać mapowanie zdarzeń korelacyjnych na platformie programistycznej Mitre ATT&CK;
- 22) system w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email;
- 23) rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE;
- 24) wbudowane mechanizmy detekcji zagrożeń pozwalają na szybkie reagowanie na potencjalne ataki;
- 25) integracja się z różnymi źródłami logów, zarówno systemowymi, jak i aplikacyjnymi;
- 26) zapewnia normalizację logów, co ułatwia analizę i porównywanie informacji pochodzących z różnych źródeł;
- 27) posiadanie system detekcji włamań (HIDS), który monitoruje aktywność systemu operacyjnego i aplikacji na poziomie hosta;
- 28) wykrywanie podejrzanych aktywności, takich jak próby włamań, ataki brute-force czy nieautoryzowane zmiany w plikach systemowych;

- 29) posiadanie funkcji detekcji na poziomie sieci (NIDS), które monitorują ruch sieciowy i identyfikują potencjalne zagrożenia;
 - 30) analizowanie ruchu w czasie rzeczywistym, a także przeszukiwanie archiwalnych danych;
 - 31) centralne zarządzanie konfiguracją;
 - 32) umożliwianie jednolitej konfiguracji dla wielu agentów w środowisku;
 - 33) funkcje raportowania i wizualizacji, które pozwalają na szybkie zrozumienie stanu bezpieczeństwa w organizacji;
 - 34) możliwość tworzenia niestandardowych raportów i widoków;
 - 35) wbudowany system monitorowania integralności plików sprawdzający, czy pliki systemowe i konfiguracyjne nie uległy nieautoryzowanym zmianom;
 - 36) możliwość konfiguracji zautomatyzowanych reakcji na wykryte zagrożenia, co przyspiesza proces reagowania na incydenty;
 - 37) obsługiwane różne protokoły bezpieczeństwa, takie jak Syslog, SNMP;
 - 38) moduły i rozszerzenia, które umożliwiają dostosowanie systemu do specyficznych potrzeb organizacji;
 - 39) system musi umożliwiać generowanie raportów na żądanie oraz raportów okresowych;
 - 40) raporty powinny być konfigurowalne i dostosowane do potrzeb różnych grup odbiorców;
 - 41) system musi zapewniać bezpieczne przechowywanie zebranych logów i zdarzeń przez określony czas – min. 12 miesięcy;
 - 42) dane powinny być chronione przed nieautoryzowanym dostępem i modyfikacją.
- b) Wymagania niefunkcjonalne systemu SIEM:
- 1) wydajność: system SIEM musi zapewniać wysoką wydajność i skalowalność, aby obsłużyć dużą ilość danych i zdarzeń.
 - 2) bezpieczeństwo: system SIEM musi spełniać wysokie standardy bezpieczeństwa, w tym szyfrowanie danych w transzycie i w spoczynku.
 - 3) łatwość użycia: Interfejs użytkownika systemu SIEM powinien być intuicyjny i łatwy w obsłudze.
- c) Wykonawca opracuje projekt techniczny realizacji uzgodnionej koncepcji, uwzględniający najlepsze praktyki i rekomendacje wdrożenia systemu SIEM. W projekcie technicznym muszą być zawarte:
- 1) Architektura wdrożenia
 - 2) Usługi i systemy monitorowanie przez SIEM
 - 3) Wykaz logów zbieranych przez SIEM
 - 4) Wykaz wymaganych przez system SIEM portów
 - 5) Opcje instalacji agentów SIEM
 - 6) Opcje podłączenia urządzeń sieciowych do SIEM
 - 7) Szczegółowy harmonogram realizacji prac, uwzględniający specyfikę organizacji Zamawiającego
- d) Wykonawca wykona instalację i konfigurację rozwiązania SIEM w tym:
- 1) Instalację SIEM w dostarczonej przez Wykonawcę infrastrukturze IaaS
 - 2) Konfigurację portów wymaganych przez SIEM
 - 3) Instalację agenta SIEM na systemach Windows
 - 4) Instalację agenta SIEM na systemach Linux
 - 5) Utworzy reguły dla poszczególnych grup agentów
 - 6) Podłączy urządzenia sieciowe do SIEM
 - 7) Dostosuje reguły zbierania logów z urządzeń
 - 8) Dostosuje reguły zbierania logów z systemów Windows

- 9) Dostosuje reguły zbierania logów z systemów Linux
 - 10) Utworzy reguły normalizacji logów, jeśli będzie taka potrzeba
 - 11) Skonfiguruje moduł integralności plików oraz rejestru na systemach Windows monitorowanych przez SIEM
 - 12) Utworzy reguły wykrywania ataków
 - 13) Utworzy reguły wykrywania ataków Pass-the-Hash
 - 14) Utworzy reguły wykrywania ataków Pass-the-ticket
 - 15) Utworzy reguły wykrywania ataków DCSync
 - 16) Utworzy reguły wykrywania ataków Golden Ticket
 - 17) Utworzy reguły wykrywania ataków Kerberoasting
 - 18) Utworzy reguły wykrywania ataków na poświadczenia Windows
 - 19) Utworzy reguły wykrywania ataków na bazę haseł z Ntds.dit
 - 20) Utworzy reguły wykrywania połączeń PsExec w systemach Windows
 - 21) Utworzy reguły wykrywania ataków Ransomware
 - 22) Skonfiguruje listy IP allow i IP block dla systemu SIEM
 - 23) Uruchomi moduł wykrywający podatności CVE na systemach monitorowanych przez SIEM
 - 24) Skonfiguruje moduł wykrywający poziom bezpieczeństwa na systemach monitorowanych przez SIEM
- e) Wykonawca zapewni wsparcie techniczne oraz serwis systemu SIEM przez okres nie krócej niż do 31.12.2026. Wsparcie powinno obejmować dostęp do aktualizacji oprogramowania oraz pomoc w rozwiązywaniu problemów i dostosowywaniu systemu.
- f) Zamawiający oczekuje, że infrastruktura IT Zamawiającego objęta będzie monitoringiem SOC.
- g) Wykonawca w ramach realizacji zamówienia zapewni własną infrastrukturę teleinformatyczną wraz z niezbędnym oprogramowaniem do świadczenia ochrony SOC, m.in.: przestrzeń dyskową na potrzeby zbierania logów, serwery wirtualne, oprogramowanie oraz inne niezbędne zasoby do prawidłowego świadczenia usługi.

Dostarczenie platformy do zarządzania zdarzeniami bezpieczeństwa

Wymagania funkcjonalne dla platformy zarządzania zdarzeniami bezpieczeństwa:

- 1) Rozwiązanie musi mieć możliwość integracji z dostarczonym systemem SIEM oraz musi być automatycznie zasilane informacjami z systemu SIEM
- 2) Rozwiązanie musi być hostowane w infrastrukturze IaaS wykonawcy spełniającej minimalne wymagania bezpieczeństwa opisane w OPZ
- 3) Rozwiązanie musi zawierać dwa moduły, dla zespołu SOC Zamawiającego oraz Zamawiającego.
- 4) Moduł dla Zamawiającego:
 - a. lista aktualnie obsługiwanych case'ów przez zespół cyberbezpieczeństwa, z możliwością śledzenia postępów i statusów
 - b. wizualizacja zidentyfikowanych podatności w organizacji klienta z podziałem na kategorie według krytyczności z podziałem na low, medium, high, critical
 - c. raportowanie - umożliwiający pobranie raportu dziennego lub miesięcznego zawierającego szczegółowe podsumowanie statystyk dotyczących alertów, case'ów oraz zablokowanych ataków. Raport obejmuje także podział obsługiwanych case'ów na True Positive (prawdziwe zagrożenia) oraz False Positive (fałszywe alarmy). Dodatkowo, zawiera informacje o wykrytych podatnościach, z podziałem na kategorie według krytyczności: critical, high, medium oraz low.

d. Zablokowane ataki - szczegółowe statystyki dotyczące zablokowanych ataków na infrastrukturę organizacji z możliwością analizy trendów i identyfikacji najczęstszych zagrożeń

5) Moduły dla zespołu SOC Zamawiającego:

a. Panel obsługi CASE umożliwiający kompleksową obsługę każdego incydentu (CASE) i oferuje następujące funkcje:

- oznaczenie aktualnego statusu obsługi CASE: Unspecified, In Progress, Close,
- przypisanie osoby odpowiedzialnej za obsługę danego incydentu,
- zdefiniowanie priorytetu: Low, Medium, High, Critical,
- oznaczenie, czy CASE wymaga standardowej reakcji, czy priorytetowej (szybkiej) reakcji,
- określenie rozwiązania CASE: False Positive lub True Positive,
- powiadomienie mail lub sms o postępie lub zakończeniu obsługi CASE,
- logowanie czasu poświęconego na obsługę CASE,
- możliwość utworzenia ticketu w systemie zgłoszeniowym (np. Jira, ServiceNow),
- możliwość dodawania notatek z możliwością formatowania oraz załączników,
- dodawanie wskaźników kompromitacji (IoC) do każdego incydentu oraz ich analiza, umożliwienie na ręczne tworzenie CASE, jeśli nie zostały one wygenerowane automatycznie, a następnie postępowanie z nimi w podobny sposób, jak z alertami pochodzącymi z systemu SIEM.

6) Panel administratora:

- szczegółowy przegląd obsługiwanych Case'ów przez operatorów SOC,
- podgląd średniego czasu reakcji na incydent (CASE) przez operatorów SOC,
- konfiguracja interwałów czasowych dla alertów generowanych przez system SIEM, pozwala na określenie częstotliwości, z jaką CASE będą tworzone,
- configure excepted IPs – definiowanie wykluczonych adresów IP (tzw. whitelist) w celu pominięcia alertów dla zaufanych adresów w monitoringu,
- define SOC service info – definiowanie treści informacyjnych dla Zamawiającego,
- my cases - podgląd aktualnie przypisanych CASE do zalogowanego użytkownika,
- all cases - podgląd zbiorczy wszystkich CASE.

Dostarczenie połączeń sieciowych

1. Wykonawca ma obowiązek dostarczyć na potrzeby zadań połączenia telekomunikacyjne i sieciowe pozwalające na płynne działanie wszystkich systemów i rozwiązań umieszczonych w środowisku teleinformatycznych Wykonawcy, w tym:

a. do środowiska IaaS - zapewnić połączenia do sieci Internet za pomocą co najmniej 2 niezależnych operatorów telekomunikacyjnych o zasięgu co najmniej krajowym o przepustowości symetrycznej nie mniejszej niż 1 Gbps,

b. zapewnić ochronę 24/7/365 przed atakami DDoS w pełnym zakresie przepustowości dla dostarczanych łącz, o których mowa w pkt. 1) powyżej,

c. do środowiska IaaS - zapewnić połączenia między VM na interfejsach co najmniej 10G Ethernet. Każdy serwer fizyczny używany do wystawienia zasobów w ramach środowiska teleinformatycznego IaaS musi być połączony dwoma niezależnymi drogami, do dwóch niezależnych przełączników sieciowych, co najmniej 1 połączeniem 10G Ethernet na każdej drodze. Połączenia do macierzy dyskowych muszą być zrealizowane na portach co najmniej 10G FC lub równoważnych. Każda macierz używana do wystawienia zasobów w ramach środowiska teleinformatycznego musi być połączona dwoma niezależnymi drogami, do dwóch niezależnych przełączników sieciowych FC, co najmniej 2 połączeniami 10G FC lub równoważnymi.

d. Komunikacja do infrastruktury Zamawiającego musi się odbywać po zabezpieczonym kanale VPN dla systemu SIEM, oraz HTTPS dla usługi kopii zapasowej.

Wymogi w zakresie bezpieczeństwa infrastruktury PDC

1. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) Zamawiający wymaga od Wykonawcy uruchomienia i wdrożenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej wraz z zapewnieniem rozwiązań w obszarze bezpieczeństwa i ochrony przed cyberzagrożeniami w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw.
2. Z uwagi na potrzebę wysokiej dostępności całej infrastruktury będącej przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający oczekuje, aby proponowane rozwiązanie spełniało najwyższe, dostępne na terenie Unii Europejskiej standardy bezpieczeństwa teleinformatycznego. Zamawiający na etapie wyboru oferty, a także realizacji umowy zastrzega możliwość weryfikacji i wezwania Wykonawcy do udokumentowania spełniania każdego z wymogów określonych poniżej:
 - 1) PDC posiada odpowiednie zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych Zamawiającego. Wykonawca ponosi odpowiedzialność w zakresie bezpieczeństwa informacji i danych przechowywanych na wykorzystanej infrastrukturze teleinformatycznej PDC,
 - 2) PDC posiadają zabezpieczenia sprzętu teleinformatycznego w postaci:
 - a) izolacji sprzętu krytycznego (dedykowana przestrzeń wyłącznie dla urządzeń serwerowych),
 - b) ochrony przed uszkodzeniem infrastruktury serwerowej w postaci zamykanych szaf rack,
 - c) prowadzenia rejestru wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego,
 - d) ochrony przed dostępem dla osób nieupoważnionych w trybie 24/7,
 - e) ochrony świadczonej przez licencjonowaną firmę ochroniarską w trybie 24/7,
 - 3) PDC realizuje profesjonalne utrzymanie i konserwację posiadanej infrastruktury teleinformatycznej w postaci:
 - a) posiadania i stosowania procedury kontroli, regularnych przeglądów zgodnie z zaleceniami producentów, konserwacji i naprawy sprzętu teleinformatycznego, energetycznego i klimatyzacyjnego,
 - b) napraw dokonywanych przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami lub autoryzowane serwisy zewnętrzne,
 - c) usuwaniem nośników danych ze sprzętu teleinformatycznego przed przekazaniem do naprawy lub serwisu,
 - d) stosowania bezpiecznej utylizacji lub przekazywania sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi),
 - e) prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.
 - 4) PDC spełnia wymagania bezpieczeństwa w zakresie parametrów powalających wyeliminować wskazane zagrożenia:

Parametr	Wyeliminowanie zagrożenia
Obiekt i lokalizacja	
PDC zlokalizowane na terenie UE, a wszystkie dane Zamawiającego będą gromadzone i przetwarzane wyłącznie na terenie UE lub Lichtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienia wymagań RODO / GDPR.
PDC posiada ogrodzony zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).
PDC jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury.
PDC jest oddalony nie mniej niż 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). Zagrożenie fizycznego uszkodzenia infrastruktury IT oraz innych urządzeń w skutek eksplozji zewnętrznej.
PDC nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi.	Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).
PDC spełnienia wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie: budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.
Węzły telekomunikacyjne	
PDC posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym nie mniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego.

Dojścia połączeń PDC wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
PDC posiada węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP oraz ochroną DDoS.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.
PDC posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.
Zasilanie energetyczne	
PDC posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
PDC posiada nie mniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.
PDC posiada system zasilania awaryjnego UPS osobno na każdą linię zasilającą.	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.
PDC posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
System zasilaczy awaryjnych UPS w PDC gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich synchronizacji z siecią energetyczną.	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.
Agregaty prądotwórcze PDC posiadają zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.

najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	
Bezpieczeństwo	
PDC jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
PDC posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
PDC posiada system CCTV, który zapewnia ciągły 24/7 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.
System CCTV w PDC powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.
System SKD (System Kontroli Dostępu) w PDC obejmuje nie mniej niż trzy strefy dostępu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie.
Dostęp do strefy I (teren w otoczeniu obiektu) w PDC podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
Dostęp do strefy II (strefa technologiczna) w PDC możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
Dostęp do strefy III (pomieszczenia ze sprzętem serwerowym Zamawiającego) w PDC możliwy jest wyłącznie przy	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.

użyciu łącznie 2 elementów identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	
PDC posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
PDC posiada ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.
Monitoring	
PDC posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
PDC posiada stałe i całodobowe 24/7 monitorowanie poprawności pracy infrastruktury i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.

Wymogi w zakresie SLA i czasu reakcji

1. Z uwagi na potrzebę wysokiej dostępności usług będących przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający wymaga, aby rozwiązanie spełniało wysoki poziom SLA zaoferowany przez Wykonawcę tj. gwarancja dostępności usługi nie niższą niż SLA na poziomie dostępności 99,9% skali roku, licząc od daty zawarcia Umowy, w tym:
 - 1) obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 8/5 w godzinach 8-16,
 - 2) przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 8/5 w godzinach 8-16 w sposób autoryzowany w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status, wraz z historią wszystkich zgłoszeń,
 - 3) Czas reakcji na zgłoszenie musi wynosić nie więcej niż 60 minut od przyjęcia zgłoszenia,
 - 4) Czasy reakcji na analizy zdarzeń bezpieczeństwa muszą być realizowane zgodnie z czasami wskazanymi w Umowie.

Harmonogram realizacji uruchomienia i świadczenia usługi

1. Rozpoczęcie prac nastąpi z chwilą podpisania Umowy.
2. Uruchomienie przedmiotu zamówienia, o którym mowa tj. przygotowanie i uruchomienie infrastruktury IaaS wraz z środowiskiem dodatkowym i systemem kopii zapasowych musi zostać wykonane w terminie wskazanym w ofercie przez Wykonawcę ale nie później niż 30

dni kalendarzowych od dnia podpisania Umowy, z tym zastrzeżeniem, że uruchomienie systemu musi zostać wykonane w terminie wskazanym w ofercie przez Wykonawcę ale nie później niż 30 dni kalendarzowych od podpisania umowy.

3. Wykonawca zgłosi gotowość do obioru na 1 dzień kalendarzowy przed terminem zakończenia prac.
4. Zamawiający w ciągu 7 dni kalendarzowych jest zobowiązany do dokonania odbioru lub zgłoszenia uwag i wyznaczenia terminu na ich usunięcie, po czym przystąpi do ponownego odbioru.

Dokumentacja techniczna

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do opracowania dokumentacji powykonawczej z wdrożenia w terminie do 30 dni kalendarzowych od dnia uruchomienia usługi.
2. Dokumentacja musi zawierać co najmniej:
 - 1) Raport przedwdrożeniowy, analiza infrastruktury Zamawiającego,
 - 2) Raport powdrożeniowy, zawierający zestawienie urządzeń podłączonych do monitoringu, opis zrealizowanych prac, architekturę usługi SOC, schemat komunikacji z Zamawiającym do obsługi zdarzeń bezpieczeństwa,

Zobowiązania Wykonawcy

1. Wykonawca udzieli Zamawiającemu pełnej informacji na temat stanu realizacji przedmiotu zamówienia, na każde wezwanie Zamawiającego.
2. Wykonawca zobowiązany będzie współdziałać z osobami wskazanymi przez Zamawiającego.

Zobowiązania Zamawiającego

1. Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji przedmiotu zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji przedmiotu zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3. Zapewnienie, że dostarczone przez Zamawiającego informacje będą prawdziwe i kompletne.
4. Wsparcie w instalacji agentów monitoringu systemu SIEM
5. Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją projektu, jeśli będą one miały związek z realizacją przedmiotu zamówienia przez Wykonawcę.
6. Konsultowanie i uzgadnianie wdrażanego systemu zgodnie z wymaganiami OPZ.

Oświadczenie Wykonawcy.

Oświadczam, że składając ofertę świadom jestem jej złożenia i zapewniam, że wykonam zamówienie zgodnie z oczekiwaniami Zamawiającego.

Składając ofertę oświadczam, że spełniam warunki udziału w postępowaniu.

Oświadczam, że wykonam zamówienie zgodnie z wymaganiami zawartymi w niniejszym Opisie Przedmiotu Zamówienia.

....., dnia