Załącznik nr 1 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonanie usług w chmurze obliczeniowej typu SOCaaS dotyczących bezpieczeństwa systemów teleinformatycznych świadczonych przez Operacyjne Centrum Cyberbezpieczeństwa – SOC dla Urzędu Miasta i Gminy Piaseczno

w ramach Projektu „Cyberbezpieczna Gmina Piaseczno" dofinansowanego ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Główny kod CPV:
48421000-5 – Pakiety oprogramowania do zarządzania urządzeniami
72511000-0 – Usługi zarządzania oprogramowaniem sieciowym

a

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

SPIS TREŚCI

1. [WS] WSTĘP

Zamówienie jest realizowane w ramach projektu „Cyberbezpieczna Gmina Piaseczno" (skrót CGP))" dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Przedmiot zamówienia obejmuje wykonanie usług w chmurze obliczeniowej typu SOCaaS dotyczących bezpieczeństwa systemów teleinformatycznych świadczonych przez Operacyjne Centrum Cyberbezpieczeństwa – SOC, do których należą:
a) monitorowanie i wykrywanie incydentów bezpieczeństwa informacji;
b) reagowanie na incydenty bezpieczeństwa;
c) przeprowadzanie analiz incydentów i rekomendowanie działań naprawczych.

W ramach OPZ użyto następujące rodzaje wymagalności parametrów funkcjonalnych i organizacyjnych:
- "MUSI BYĆ" - brak spełnienia wymagania może stanowić podstawę do odrzucenia oferty lub rozwiązania umowy,
- "OPCJONALNE" - brak spełnienia wymagania nie stanowi podstawy do odrzucenia oferty,
- "PUNKTOWANE" - spełnienia wymagania jest stanowi podstawę do naliczenia dodatkowych punktów na etapie oceny ofert zgodnie z kryteriami określonymi w zapytaniu ofertowym.
Zamawiający informuje, że wszelkie wskazane w OPZ wymagania dotyczące niniejszego postępowania, w szczególności: normy, specyfikacje techniczne, nazwy własne, numery katalogowe, znaki towarowe, patenty lub pochodzenie, źródła lub szczególne procesy, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, mają charakter przykładowy.
Zostały one przywołane jedynie w celu sprecyzowania parametrów i wymogów techniczno-użytkowych przedmiotu zamówienia, Zamawiający dopuszcza materiały, urządzenia i technologie równoważne. Wszelkie materiały, urządzenia i rozwiązania równoważne, muszą spełniać następujące wymagania i standardy w stosunku do oprogramowania, urządzenia i rozwiązania wskazanego jako przykładowy, tj. muszą być co najmniej:
1. tego samego charakteru użytkowego (tożsamość funkcji),
2. tej samej charakterystyki materiałowej (rodzaj i jakość materiałów),
3. tych samych parametrów technicznych (wytrzymałość, trwałość, itp);
4. tych samych parametrów bezpieczeństwa użytkowania;
oraz muszą być
5. kompatybilne z istniejącą infrastrukturą Zamawiającego,
6. spełniać te same funkcje,
7. posiadać stosowne dokumenty dopuszczające do stosowania certyfikaty, atesty i aprobaty techniczne.
Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia.

Zamówienie powinno zostać zrealizowane z uwzględnieniem wymagań funkcjonalnych i organizacyjnych opisanych w poniższych rozdziałach, które należy traktować jako minimalne parametry do rozwiązań równoważnych.

2. [WO] WYMAGANIA OGÓLNE DOSTAWCY SOC

Wszystkie wymagania szczegółowe w zakresie zespołu SOC podlegają weryfikacji Zamawiającego w dowolnym momencie prowadzenia postępowania oraz podczas realizacji umowy. Dostawca SOC, musi spełniać następujące wymagania zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (dalej Rozporządzenie):

Lp.	ID	Nazwa wymagania	Wymagalność
2.1.	WO_017	Posiadanie i udostępnianie systemu informatycznego SIEM, który zbiera logi i zdarzenia z urządzeń i systemów organizacyjnych Zamawiającego oraz na podstawie analizy generuje alerty bezpieczeństwa, które zespół SOC musi analizować oraz reagować w celu minimalizacji ryzyka ataku.	MUSI BYĆ
2.2.	WO_003	Posiadanie wdrożonej strategii reagowania na incydenty bezpieczeństwa wraz z procedurami udostępnionymi do wglądu przez Zamawiającego na jego żądanie.	MUSI BYĆ
2.3.	WO_004	Zapewnienie wsparcia i monitorowania Zamawiającego przez całą dobę, w każdy dzień tygodnia (24/7), potwierdzone odpowiednim poziomem zatrudnienia.	MUSI BYĆ
2.4.	WO_005	Posiadanie odpowiednio przygotowanych pomieszczeń pozwalających na zapewnienie świadczenia usługi 24/7, które są wyposażone w odpowiednie środki techniczne w postaci sprzętu i oprogramowania zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo. Zamawiający na etapie przed podpisaniem umowy lub jej realizacji może zweryfikować podczas wizji lokalnej dysponowanie Wykonawcy odpowiednimi warunkami lokalizacyjnymi lub poprzez weryfikację certyfikatów potwierdzających odpowiednie warunki lokalowe (0 pkt. / 20 pkt.)	PUNKTOWANE
2.5.	WO_006	Dysponowanie redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi.	MUSI BYĆ
2.6.	WO_007	Posiadanie systemu kontroli dostępu obejmującego wszystkie wejścia i wyjścia obszaru SOC, w którym co najmniej rozpoznanie osoby uprawnionej następuje w wyniku odczytu identyfikatora lub odczytu cech biometrycznych.	MUSI BYĆ
2.7.	WO_008	Posiadanie systemu sygnalizacji napadu i włamania, stale monitorowanego przez personel bezpieczeństwa wyposażonego w rezerwowe źródło zasilania, obejmującego ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizującego co najmniej: otwarcie drzwi, poruszanie się w chronionym obszarze, stan systemu, w tym generujący ostrzeżenia i alarmy.	MUSI BYĆ
2.8.	WO_009	Posiadanie systemu sygnalizacji pożarowej obejmującego urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze.	MUSI BYĆ
2.9.	WO_016	Posiadanie zespołu, który musi obejmować minimalnie 6 osób, w szczególności wykonujących role potwierdzone certyfikatami: 1. kierownik zespołu, 2. analityk bezpieczeństwa, 3. inżynier bezpieczeństwa, 4. architekt bezpieczeństwa, 5. personel Informatyki śledczej. Dołączyć wykaz osób pracujących w Zespole SOC	MUSI BYĆ
2.10.	WO_010	Posiadanie co najmniej jednego Certyfikowanego Audytora wiodącego PN-EN ISO/IEC 27001. Certyfikat jest wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
2.11.	WO_011	Posiadanie co najmniej jednego certyfikowanego audytora CISA-ISACA, aby utrzymywać wysoki poziom bezpieczeństwa we współpracy z Zamawiającym.	MUSI BYĆ
2.12.	WO_012	Posiadanie co najmniej dwóch certyfikowanych architektów bezpieczeństwa cybernetycznego - pozwalających na stałe wsparcie w podnoszeniu poziomu bezpieczeństwa infrastruktury Zamawiającego.	MUSI BYĆ
2.13.	WO_013	Posiadanie co najmniej czterech certyfikowanych analityków bezpieczeństwa cybernetycznego pozwalających zagwarantować 1 stanowisko analityka w trybie pracy SOC 24/7, posiadane certyfikaty analityków powinny dotyczyć oferowanego systemu monitoringu.	MUSI BYĆ
2.14.	WO_001	Posiadanie ważnego certyfikatu ISO 27001 potwierdzającego bezpieczne przetwarzanie danych Klienta w całym ich zakresie.	MUSI BYĆ
2.15.	WO_002	Posiadanie ważnego certyfikatu ISO 22301 potwierdzającego posiadanie i możność realizacji procesów pozwalających utrzymać wszystkie działania SOC w deklarowanej ciągłości działania.	MUSI BYĆ
2.16.	WO_014	Posiadanie co jednego / dwóch lub więcej pracowników z certyfikatem CISSP, w celu potwierdzenia poziomu dojrzałości bezpieczeństwa dostawcy (0 pkt. /5 pkt.)	PUNKTOWANE
2.17.	WO_015	Posiadanie co najmniej jednego pracownika z certyfikatem Security+ w celu walidacji umiejętności zagwarantowania bezpieczeństwa (0 pkt. / 5 pkt.)	PUNKTOWANE

3. [WU] WYMAGANIA W ZAKRESIE PROWADZONYCH USŁUG SOC

SOC - Operacyjne Centrum Cyberbezpieczeństwa świadczące usługi w chmurze obliczeniowej typu SaaS dotyczącej bezpieczeństwa systemów teleinformatycznych. Zespół, który analizuje i monitoruje bezpieczeństwo dla organizacji oraz reaguje w razie incydentów bezpieczeństwa. Misją SOC jest ochrona Zamawiającego przed naruszeniami bezpieczeństwa poprzez identyfikację zagrożeń, analizę zdarzeń oraz reagowanie na zagrożenia i ataki cyberbezpieczeństwa. Zespół SOC powinien współpracować ze wszystkimi administratorami sieci i zespołem bezpieczeństwa Zamawiającego, zapewniając dodatkowe wsparcie techniczne i doradcze.
Poniżej opisano wymagania w zakresie świadczenia usług SOC:

Lp.	ID	Nazwa wymagania	Wymagalność
3.1.	WU_002	Zapewnienie wykonania co najmniej raz na 12 miesięcy testów penetracyjnych, pozwalających na weryfikację podatności infrastruktury Zamawiającego w celu ewaluacji zabezpieczeń.	MUSI BYĆ
3.2.	WU_004	Zespół regularnie używa i stale aktualizuje narzędzia. Zespół bez odpowiednich i aktualnych narzędzi nie może właściwie zabezpieczyć systemów i sieci.	MUSI BYĆ
3.3.	WU_005	Zespół SOC musi zbadać podejrzaną i szkodliwą aktywność w sieciach i systemach. SIEM lub oprogramowanie analityczne będzie generować alerty, które zespół następnie analizuje, bada, klasyfikuje oraz ujawnia zakres i stopień zagrożenia.	MUSI BYĆ
3.4.	WU_006	Zespół SOC prowadzi proces klasyfikacji incydentów (Alert Triage), w ramach którego SOC zapewnia zbieranie i zestawianie danych z logów wskazanych przez Zamawiającego elementów infrastruktury do których należą: serwery DELL (10 szt.), urządzenia brzegowe UTM SonicWall (1 szt.), urządzenia sieciowe zarządzalne HP (10 szt.), które pozwalają analitykom przeglądać i wykrywać zdarzenia bezpieczeństwa z dostarczonych logów. Wykaz elementów infrastruktury będzie stanowić w Załącznik nr 1 do umowy.	MUSI BYĆ
3.5.	WU_007	Zespół dokonuje priorytetyzacji incydentów (Alert Prioritization), w ramach której analitycy SOC wykorzystują swoją wiedzę o środowisku biznesowym i doświadczenie z zakresu potencjalnych zagrożeń, aby priorytetyzować alerty i decydować, które zdarzenia stanowią rzeczywiste incydenty bezpieczeństwa.	MUSI BYĆ
3.6.	WU_013	Zespół wykonuje proces naprawy i przywracania (Remediation and Recovery), co oznacza, że po wykryciu incydentu personel SOC jest odpowiedzialny za usunięcie zagrożenia, czyszczenie dotkniętych systemów i przywrócenie ich do normalnego stanu pracy.	MUSI BYĆ
3.7.	WU_014	Zespół dokonuje dokumentowania i raportowania (Post-Mortem and Reporting) z częstotliwością min. tygodniową w ramach reakcji organizacji na incydent oraz przeprowadza dodatkowe analizy kryminalistyczne w celu upewnienia się, że zagrożenie zostało w pełni zniwelowane.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

4. [WF] WYMAGANIA FUNKCJONALNE

Dostarczanie usług związanych z zapewnieniem wysokiego poziomu cyberbezpieczeństwa systemów informatycznych.

Lp.	ID	Nazwa wymagania	Wymagalność
4.1.	WF_001	SOC jest dostosowany do monitorowania dostępności i wykorzystywania infrastruktury takich jak: zasoby serwera, bazy danych, środowiska wirtualne, sieci SAN/LAN/WAN, urządzenia sieciowe, przełączniki/routery/firewalle/sondy IDP/IDS itp. oraz elementy systemu operacyjnego).	MUSI BYĆ
4.2.	WF_002	SOC stosuje się do świadczenia usługi oprogramowania klasy SIEM (Security Information and Event Management - System zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego), w którym zbierane są logi z systemów poddawane korelacji w celu wykrycia Incydentów, zwany dalej „System”.	OPCJONALNE
4.3.	WF_003	System wykorzystywany przez SOC zapewnia unikalną identyfikację każdego monitorowanego urządzenia/hosta.	MUSI BYĆ
4.4.	WF_004	System wykorzystywany przez SOC zapewnia korzystanie z mechanizmów uwierzytelniania dla Administratorów i Użytkowników.	MUSI BYĆ
4.5.	WF_005	System wykorzystywany przez SOC zapewnia wysoki poziom bezpieczeństwa komunikacji poprzez zaszyfrowanie przy użyciu protokołu TLS /SSL.	MUSI BYĆ
4.6.	WF_006	System wykorzystywany przez SOC zapewnia wysoki poziom bezpieczeństwa, w tym poufności gromadzonych danych i zapewnia ochronę przed nieautoryzowanymi zmianami.	MUSI BYĆ
4.7.	WF_007	System wykorzystywany przez SOC zapewnia graficzną prezentację wykresów z możliwością agregacji (grupowania) danych.	MUSI BYĆ
4.8.	WF_008	W przypadku przekroczenia limitów parametrów określonych przez Administratora Systemu w szczególności: wykorzystania procesora, przestrzeni dyskowej, RAM-u w przypadku maszyn wirtualnych i innych zasobów serwerów, monitoring zaalarmuje Zamawiającego, przedstawiając zagrożenia na Dashboardzie oraz umożliwi: a. Wysyłanie wiadomości e-mail b. Uruchamianie skryptu zewnętrznego.	MUSI BYĆ
4.9.	WF_009	System wykorzystywany przez SOC zapewnia niezależną konfigurację wyglądu alarmów, systemów alarmowych oraz sposobu ich prezentacji.	MUSI BYĆ
4.10.	WF_010	System wykorzystywany przez SOC zapewnia raportowanie zdarzeń, w tym incydentów, poziomu wykorzystania infrastruktury oraz zasobów wykorzystywanych w infrastrukturze Zamawiającego.	MUSI BYĆ
4.11.	WF_011	System wykorzystywany przez SOC zapewnia generowanie raportów w oparciu o zaplanowany harmonogram na dany okres w zakresie stanu hostów i usług oraz udostępnianie go za pośrednictwem poczty elektronicznej.	MUSI BYĆ
4.12.	WF_012	System wykorzystywany przez SOC dostarcza predefiniowanych widoków prezentujących stan monitorowanej infrastruktury w szczególności: zużycie dysku, RAM-u w maszynach wirtualnych oraz zużycie procesora.	MUSI BYĆ
4.13.	WF_013	System wykorzystywany przez SOC zapewnia wgląd w budowę struktury hierarchicznej, pozwalającej na przejście "od ogółu do szczegółu" (tzw. funkcjonalność "drilldown"); Funkcjonalność ta ma pozwolić na konstruowanie ogólnych widoków prezentujących aktualny stan monitorowanej infrastruktury w sposób wysokopoziomowy, a jednocześnie pozwolić na szybkie wyświetlanie bardziej szczegółowych widoków, np. dotyczących konkretnej monitorowanej lokalizacji lub urządzenia.	OPCJONALNE
4.14.	WF_014	System wykorzystywany przez SOC zapewnia, że Szablony raportów dostarczane w ramach oprogramowania monitorującego (domyślne i utworzone przez użytkownika) muszą zapewniać parametryzację, m. in. minimalne definiowanie zakresu czasu lub listę interfejsów.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
4.15.	WF_015	System wykorzystywany przez SOC ma możliwość tworzenia własnych raportów i udostępniania ich w formie szablonów innym Użytkownikom. Narzędzie do raportowania musi mieć intuicyjny interfejs graficzny.	MUSI BYĆ
4.16.	WF_016	System wykorzystywany przez SOC zapewnia możliwości generowania raportów w standardowych formatach, minimum: PDF, CSV i XLS.	MUSI BYĆ
4.17.	WF_017	System wykorzystywany przez SOC umożliwia korzystanie ze skryptów napisanych przez pracowników Zespołu SOC w celu monitorowania strony internetowej/hosta.	MUSI BYĆ
4.18.	WF_018	System wykorzystywany przez SOC ma możliwość wskazania Użytkownika lub grupy Użytkowników, do których wysyłana będzie wiadomość dotycząca hosta/usługi lub grupy hostów/usług na podstawie zdefiniowanych filtrów do wysyłania powiadomień.	MUSI BYĆ
4.19.	WF_019	System wykorzystywany przez SOC zapewnia integrację z systemami uwierzytelniania opartymi na usługach katalogowych, minimum Active Directory oraz LDAP.	MUSI BYĆ
4.20.	WF_020	System wykorzystywany przez SOC zapewnia możliwość pracy dla wielu niezależnych profili użytkowników, na których można zdefiniować niezależną konfigurację dla dostępnych widoków generujących raporty z hostów, w celu zapewnienia ograniczonego dostępu do danych klienta.	MUSI BYĆ
4.21.	WF_021	System zapewnia monitorowanie parametrów prawidłowego funkcjonowania serwerów, systemów operacyjnych, baz danych i urządzeń Sieci SAN / LAN.	MUSI BYĆ
4.22.	WF_022	System wykorzystywany przez SOC zapewnia monitorowanie pracy maszyn wirtualnych, logów systemowych oraz aktywności usług i użytkowników na maszynach wirtualnych.	MUSI BYĆ
4.23.	WF_023	System wykorzystywany przez SOC umożliwia monitorowanie procesów działających na danej jednostce oraz modyfikacji plików i logowań w systemach Linux i Windows.	MUSI BYĆ
4.24.	WF_024	System wykorzystywany przez SOC umożliwia monitorowanie co najmniej następujących baz danych: Oracle, Microsoft SQL Server.	MUSI BYĆ
4.25.	WF_025	System wykorzystywany przez SOC umożliwia monitorowanie w szczególności następujących systemów operacyjnych: Windows Server 2022, Windows Server 2019, Windows Server 2016, Oracle, Linux, Centos, Red Hat.	MUSI BYĆ