Ogłoszenie o wyniku postępowania
Dostawy
Wdrożenie i uruchomienie systemu klasy SIEM open-source w modelu on-premise

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego
Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: GMINA CELESTYNÓW

1.4) Krajowy Numer Identyfikacyjny: REGON 013268965

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Regucka 3

1.5.2.) Miejscowość: Celestynów

1.5.3.) Kod pocztowy: 05-430

1.5.4.) Województwo: mazowieckie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL912 - Warszawski wschodni

1.5.9.) Adres poczty elektronicznej: zamowienia@celestynow.pl

1.5.10.) Adres strony internetowej zamawiającego: www.celestynow.pl

1.6.) Adres strony internetowej prowadzonego postępowania:
https://celestynow.logintrade.net/rejestracja/ustawowe.html

1.7.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.8.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:
Wdrożenie i uruchomienie systemu klasy SIEM open-source w modelu on-premise

2.4.) Identyfikator postępowania: ocds-148610-6b2f923d-cf48-4a0a-aefa-c4e3072eb545

2.5.) Numer ogłoszenia: 2026/BZP 00461722

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-09-29

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2026/BZP 00044283/04/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.2 Podniesienie poziomu cyberbezpieczeństwa w Gminie Celestynów z podziałem na części.

2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.12.) Nazwa projektu lub programu:
8. Przedmiot zamówienia współfinansowany jest przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa,

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy:

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy: Tak

2.14.) Numer ogłoszenia: 2026/BZP 00331389

SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: RIZPiFZ.271.40.2026

4.2.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.4.) Rodzaj zamówienia: Dostawy

4.5.1.) Krótki opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest wdrożenie systemu klasy SIEM open-source w modelu on-premise, obejmującego agentowe monitorowanie komputerów oraz bezagentowe monitorowanie urządzeń infrastrukturalnych w Urzędzie Gminy Celestynów, w ramach zadania inwestycyjnego pn. ,,Podniesienie poziomu cyberbezpieczeństwa w Gminie Celestynów”.
2. Przedmiot zamówienia obejmuje wykonanie usług projektowych, wdrożeniowych, instalacyjnych i konfiguracyjnych polegających na wdrożeniu systemu klasy SIEM (Security Information and Event Management) w wersji open-source, działającego w modelu on-premise, przeznaczonego do monitorowania zdarzeń bezpieczeństwa w infrastrukturze IT Zamawiającego, wraz z konfiguracją zbierania logów, analizą zdarzeń, przygotowaniem reguł detekcji oraz dokumentacją powdrożeniową.
3. Celem zamówienia jest wdrożenie centralnego systemu monitorowania bezpieczeństwa, umożliwiającego zbieranie, analizę i korelację zdarzeń z systemów IT, wykrywanie incydentów bezpieczeństwa, zwiększenie poziomu nadzoru nad infrastrukturą oraz poprawę zdolności reagowania na zagrożenia.
4. Zakres przedmiotu zamówienia obejmuje:
1) analizę przedwdrożeniową obejmującą identyfikację źródeł logów, zakres monitorowania oraz wymagania techniczne środowiska Zamawiającego,
2) instalację i konfigurację systemu klasy SIEM open-source w modelu on-premise w środowisku Zamawiającego,
3) przygotowanie i uruchomienie systemu na maszynie wirtualnej zgodnej ze standardem Proxmox (dostarczonej przez Wykonawcę lub wdrożonej na infrastrukturze Zamawiającego),
4) konfigurację komponentów systemu odpowiedzialnych za:
a) zbieranie logów,
b) korelację zdarzeń,
c) analizę bezpieczeństwa,
d) generowanie alertów,
e) prezentację danych (interfejs webowy),
5) konfigurację agentowego monitorowania komputerów (maksymalnie 50 stacji roboczych), w tym:
a) przygotowanie pakietów instalacyjnych,
b) instalację i konfigurację agentów,
c) weryfikację poprawności komunikacji,
d) zbieranie logów systemowych oraz zdarzeń bezpieczeństwa,
6) konfigurację bezagentowego monitorowania urządzeń infrastrukturalnych (maksymalnie 100urządzeń), w szczególności:
a) urządzeń sieciowych,
b) zasilaczy UPS,
c) innych urządzeń generujących logi,
7) konfigurację zbierania logów z wykorzystaniem standardowych protokołów (np. syslog, SNMP, inne dostępne mechanizmy),
8) przygotowanie i wdrożenie podstawowego zestawu reguł detekcji zdarzeń bezpieczeństwa, obejmujących co najmniej:
a) nieudane próby logowania,
b) próby eskalacji uprawnień,
c) anomalie w ruchu systemowym,
d) zdarzenia związane z integralnością systemu,
e) podstawowe zdarzenia związane z bezpieczeństwem systemów operacyjnych,
9) konfigurację alertów i powiadomień (np. e-mail lub inne dostępne mechanizmy),
10) przygotowanie dashboardów i widoków umożliwiających analizę zdarzeń oraz bieżący monitoring,
11) konfigurację retencji logów oraz podstawowych zasad archiwizacji danych,
12) wykonanie podstawowego utwardzenia systemu (hardening), obejmującego:
a) zabezpieczenie dostępu administracyjnego,
b) aktualizację komponentów,
c) ograniczenie zbędnych usług,
d) konfigurację polityk dostępu,
13) konfigurację mechanizmu kopii zapasowych konfiguracji systemu,

14) przeprowadzenie testów powdrożeniowych potwierdzających poprawność działania systemu, w tym:
a) poprawność zbierania logów,
b) działanie agentów,
c) generowanie alertów,
d) dostępność interfejsu zarządzającego,
15) opracowanie i przekazanie dokumentacji powdrożeniowej,
16) przeprowadzenie szkolenia administratora z zakresu obsługi i administracji systemu (minimum 4 godziny).
5. Wymagania funkcjonalne i techniczne:
1) Wdrażane rozwiązanie musi:
a) być systemem klasy SIEM w wersji open-source,
b) działać lokalnie w infrastrukturze Zamawiającego (on-premise),
c) umożliwiać centralne zbieranie i analizę logów,
d) obsługiwać agentowe monitorowanie komputerów (do 50 urządzeń),
e) obsługiwać bezagentowe monitorowanie urządzeń (do 100 urządzeń),
f) umożliwiać analizę i korelację zdarzeń,
g) umożliwiać generowanie alertów bezpieczeństwa,
h) posiadać interfejs webowy do zarządzania i analizy danych,
i) umożliwiać rozbudowę i dalszy rozwój systemu przez Zamawiającego.
2) Maszyna wirtualna powinna być zgodna ze standardem Proxmox. Parametry zasobów zostaną uzgodnione na etapie analizy, przy czym Wykonawca przedstawi wymagania minimalne i rekomendowane.
6. Wymagania wobec Wykonawcy:
1) sporządzenie i przedstawienie Zamawiającemu harmonogramu wdrożenia oraz planu realizacji prac przed rozpoczęciem czynności wdrożeniowych,
2) wykazanie, że w okresie ostatnich 3 lat przed upływem terminu składania ofert Wykonawca należycie zrealizował co najmniej dwa wdrożenia oprogramowania klasy SIEM, w tym co najmniej jedno wdrożenie na rzecz jednostki publicznej,
3) dołączenie do oferty dokumentów potwierdzających należyte wykonanie wdrożeń, o których mowa powyżej, w szczególności referencji, protokołów odbioru lub innych równoważnych dokumentów wystawionych przez podmioty, na rzecz których wdrożenia zostały wykonane,
4) zapewnienie personelu posiadającego doświadczenie w administracji systemami Linux oraz systemami monitoringu bezpieczeństwa,
5) skierowanie do realizacji zamówienia co najmniej jednej osoby posiadającej certyfikat lub potwierdzenie ukończenia szkolenia poświadczające wiedzę w zakresie wdrażanego rozwiązania SIEM,
6) dołączenie do oferty kopii certyfikatu, zaświadczenia lub innego dokumentu potwierdzającego ukończenie szkolenia z zakresu SIEM dla osoby, która będzie uczestniczyć w wykonaniu wdrożenia,
7) wykonanie wdrożenia zgodnie z dobrymi praktykami bezpieczeństwa, zasadą najmniejszych uprawnień oraz aktualnym stanem wiedzy technicznej,
8) przekazanie pełnej dokumentacji powdrożeniowej,
9) zapewnienie minimum 3-miesięcznego wsparcia powdrożeniowego,
10) Wykonawca zobowiązany jest do realizacji prac w sposób zapewniający bezpieczeństwo informacji oraz ciągłość działania Zamawiającego.
7. Odbiór prac.
1) Warunkiem odbioru będzie:
a) uruchomienie systemu SIEM w środowisku Zamawiającego,
b) działające monitorowanie agentowe (do 40 komputerów),
c) działające monitorowanie bezagentowe (do 80 urządzeń),
d) poprawne zbieranie i analiza logów,
e) skonfigurowane alerty,
f) przekazana dokumentacja,
g) przeprowadzone szkolenie.
8. Przedmiot zamówienia współfinansowany jest przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa,
9. W ofercie należy podać cenę obejmującą cały zakres przedmiotu zamówienia wynikający z niniejszego opisu, uwzględniając zapisy SWZ i warunki realizacji określone w projekcie umowy załączonym do SWZ.
10. Zamawiający nie przewiduje żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu umowy, a płatność nastąpi zgodnie z zapisami projektu umowy załączonego do SWZ.

4.5.3.) Główny kod CPV: 72263000-6 - Usługi wdrażania oprogramowania

4.5.4.) Dodatkowy kod CPV:

72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

48732000-8 - Pakiety oprogramowania do zabezpieczania danych

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się zawarciem umowy

SEKCJA VI OFERTY

6.1.) Liczba otrzymanych ofert lub wniosków: 6

6.1.3.) Liczba otrzymanych od MŚP: 6

6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0

6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0

6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 1

6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 34255,50 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 61500,00 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 34255,50 PLN

6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie

6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA

7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: AMITRONIC Amadeusz Kusz

7.3.2) Krajowy Numer Identyfikacyjny: 8771483213

7.3.3) Ulica: Gaj 32

7.3.4) Miejscowość: Łąkorz

7.3.5) Kod pocztowy: 12-334

7.3.6.) Województwo: warmińsko-mazurskie

7.3.7.) Kraj: Polska

7.4.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA

8.1.) Data zawarcia umowy: 2026-09-02

8.2.) Wartość umowy/umowy ramowej: 34255,50 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej: 30 dni