OPIS PRZEDMIOTU ZAMÓWIENIA – Wdrożenie systemu SIEM - monitoring sieci w czasie rzeczywistym

I. Zamawiający:

Województwo Opolskie z siedzibą w: Opole 45-082, przy ul. Piastowska 14
NIP: 7543077565, REGON: 531412421.

II. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wdrożenie Systemu Monitoringu zdarzeń związanych z bezpieczeństwem informatycznym (SIEM). System SIEM ma na celu detekcję, monitorowanie, analizę oraz odpowiedź na incydenty dotyczące bezpieczeństwa w infrastrukturze Zamawiającego. System powinien umożliwić integrację danych z wielu źródeł, takich jak systemy detekcji intruzów (IDS), firewalle, systemy kontroli dostępu do sieci (NAC), a także logi z serwerów i urządzeń końcowych Zamawiającego.

Zadanie realizowane jest w konkursie grantowym „Cyfrowe Województwo" realizowanym w ramach projektu „Cyfrowa Gmina". Projekt współfinansowany jest ze środków Unii Europejskiej w ramach działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU Programu Operacyjnego Polska Cyfrowa na lata 2014-2020.

III. Szczegółowe założenia specyfikacji

1. Funkcjonalność systemu:

1.1. *Monitorowanie w czasie rzeczywistym*: System musi umożliwiać śledzenie aktywności w sieci i na urządzeniach w czasie rzeczywistym, umożliwiając szybką identyfikację i reagowanie na potencjalne zagrożenia.
1.2. *Raportowanie*: System powinien oferować zaawansowane funkcje raportowania, umożliwiające generowanie szczegółowych raportów dotyczących różnych aspektów bezpieczeństwa sieci.
1.3. *Powiadomienia alarmowe*: System powinien automatycznie generować powiadomienia alarmowe w odpowiedzi na wykryte anomalie lub incydenty bezpieczeństwa.
1.4. *Analiza behawioralna i uczenie maszynowe*: System powinien wykorzystywać zaawansowane techniki analizy behawioralnej i uczenia maszynowego do identyfikacji i klasyfikacji anomalii w sieci.
1.5. Analiza bezpieczeństwa: w czasie rzeczywistym zbieranie, agregowanie, indeksowanie i analizowanie danych dotyczących bezpieczeństwa. Pomaga wykryć włamania, zagrożenia oraz wszelkie anomalie.
1.6. Wykrywanie włamań: skanuje system w poszukiwaniu złośliwego oprogramowania, rootkitów.
1.7. Analiza logów: odczyt logów, przesłanie do centralnego menagera w celu analizy i przechowywania.
1.8. Monitorowanie integralności plików: monitoruje system plików, identyfikuje zmiany w treści.
1.9. Zarządzanie podatnościami: pobieranie danych inwentaryzujących oprogramowanie i bieżące korelowanie ich z aktualizowanymi bazami danych CVE (Common Vulnerabilities and Exposures).

1.10. Ocena konfiguracji: monitorowanie ustawień konfiguracji systemu i aplikacji, aby upewnić się, że są one zgodne z przyjętymi zasadami, alerty mogą zawierać wytyczne dotyczące utwardzenia konfiguracji.
1.11. Reakcja na incydent: podjęcie reakcji na wykryty incydent bezpieczeństwa.
1.12. Bezpieczeństwo w chmurze: integracja z infrastrukturą chmury na poziomie API (AWS, Azure, GC) i zapewnienie reguł oceny konfiguracji środowiska chmurowego.
1.13. Bezpieczeństwo kontenerów: wgląd w bezpieczeństwo kontenerów Dockera.

2. Integracja:

2.1. *Integracja z systemami: System SIEM powinien 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 Zamawiającego i innymi.*
2.2. Wsparcie dla wielu protokołów: System powinien obsługiwać różne protokoły transmisji logów, takie jak Syslog, SNMP, WMI i inne.
2.3. Zbieranie i normalizacja logów: System powinien umożliwiać zbieranie, normalizację i korelację logów z różnych źródeł w jednolitym formacie.

3. Skalowalność:

3.1. Elastyczność i adaptacja: System musi być skalowalny, umożliwiając organizacji łatwe dostosowanie go do rosnących potrzeb i zmieniających się wymagań.

4. Bezpieczeństwo i prywatność:

4.1. Zgodność z regulacjami: System musi być zgodny z wszystkimi stosownymi regulacjami dotyczącymi prywatności i bezpieczeństwa, w tym z Rozporządzeniem o Ochronie Danych Osobowych (GDPR) i standardem ISO 27001.
4.2. Zasady bezpieczeństwa: System musi oferować zaawansowane funkcje bezpieczeństwa, w tym szyfrowanie danych, zarządzanie tożsamością i dostępem, monitorowanie w czasie rzeczywistym i alarmy.

5. Wsparcie i utrzymanie

5.1. Wsparcie techniczne: Dostawca powinien zapewnić wsparcie techniczne po wdrożeniu, aby pomóc organizacji w efektywnym zarządzaniu systemem i rozwiązywaniu ewentualnych problemów przez okres 12 miesięcy.
5.2. Aktualizacje i konserwacja: Dostawca powinien regularnie dostarczać aktualizacje systemu i zapewniać konserwację, aby zapewnić ciągłą ochronę przed nowymi zagrożeniami przez okres 12 miesięcy.
5.3. Dokumentacja: Dostawca powinien dostarczyć dokumentację zawierającą minimum: opis techniczny środowiska, w tym schemat blokowy systemu wraz z opisem jego składowych oraz przepływu i przetwarzania danych w systemie oraz diagram wdrożenia obejmujący wszystkie składowe systemu wraz ze ścieżkami komunikacji pomiędzy składowymi oraz systemami zewnętrznymi z opisem wykorzystywanych protokołów i portów wszystkich uruchomionych w systemie usług; opis konfiguracji systemu oraz parametrów systemu; opis zarządzania użytkownikami i uprawnieniami….

6. Szkolenia

6.1. Zarządzanie systemem: Zespół IT Zamawiającego powinien przejść szkolenie z zakresu zarządzania systemem, w tym konfiguracji, monitorowania, alarmów, raportowania i reagowania na incydenty.

IV. Wymagania dla wykonawców

1. *Doświadczenie*: Oferent musi wykazać doświadczenie w wdrażaniu i zarządzaniu systemami SIEM w środowiskach o podobnej skali i złożoności w okresie ostatnich 36 miesięcy.
2. *Certyfikaty*: Oferent musi posiadać certyfikat audytora wewnętrznego ISO 27001, co potwierdza jego zdolność do monitorowania zgodności stanu bezpieczeństwa infrastruktury z tym standardem.
3. *Referencje*: Oferent musi dostarczyć referencje od poprzednich klientów, które mogą potwierdzić jego doświadczenie.
4. *Wsparcie i utrzymanie*: Oferent powinien być w stanie zapewnić wsparcie techniczne i utrzymanie systemu po jego wdrożeniu, w tym regularne aktualizacje i konserwacje przez okres 12 miesięcy.
5. *Testowanie przed wdrożeniem*: Oferent powinien umożliwić przetestowanie systemu w realnym środowisku przed podjęciem wdrożenia.

Inne wymagania:

1. *Harmonogram*: Oferent powinien dostarczyć szczegółowy harmonogram wdrożenia, uwzględniający wszystkie kluczowe etapy, w tym konfigurację, integrację, szkolenie użytkowników systemu, testowanie i optymalizację systemu.

V. Kryteria wyboru ocen

Przy wyborze oferty do realizacji zamawiający będzie się kierował:

1. Kryterium: Cena - 70% (max. 7 punktów)
2. Kryterium: Doświadczenie osoby skierowanej do realizacji zamówienia - 30% (max. 3 punkty)

Oferta może uzyskać łącznie maksymalnie 10 punktów.

Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

VI. Termin realizacji zamówienia

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie 30 dni od dnia zawarcia umowy.

VII. Oferta ma zawierać:

1. Kompletny, wypełniony formularz ofertowy stanowiący załącznik nr 1;
2. Harmonogram opisany w pkt. IV Opisu Przedmiotu Zamówienia.
3. Dokumenty poświadczające spełnienie wymagań wobec wykonawców określone w pkt. IV Opisu Przedmiotu Zamówienia.

Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

VIII. Miejsce i termin składania ofert

Oferty proszę składać w formie elektronicznej na platformie:

https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

Termin składania ofert upływa z dniem: 30.08.2023 r. godz. 12:00.

Oferty złożone po terminie nie będą rozpatrywane.

IX. Termin związania ofertą

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą

X. Postanowienia końcowe

1. Zamawiający zastrzega sobie prawo odstąpienia, bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu publikacji niniejszego zapytania ofertowego.
2. Zapytanie może zostać zmienione przed upływem terminu składania ofert przewidzianym w zapytaniu ofertowym. Zmiana oraz treść pytań wraz z wyjaśnieniami zostanie opublikowana na stronie: https://bazakonkurencyjnosci.funduszeeuropeiskie.gov.pl

XI. Załączniki

1. Załącznik nr 1 - Formularz ofertowy
2. Załącznik nr 2 - Wzór umowy
3. Załącznik nr 3 - Klauzula informacyjna RODO