

**Załącznik Nr 1.4 do SWZ
OPZ –ZADANIE 4**

(Znak sprawy: SR.271.24.2025)

„Dostawa i wdrożenie rozwiązania SIEM „Security Information and Event Management”

w ramach projektu grantowego "Cyberbezpieczny Samorząd" współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, tytuł projektu: „Podniesienie poziomu bezpieczeństwa infrastruktury informatycznej oraz poziomu wiedzy o cyberzagrożeniach w Urzędzie Gminy Dębe Wielkie”

Wymagania Ogólne:

Przedmiotem zamówienia jest wdrożenie systemu **SIEM** (Security Information and Event Management) z modułami współpracującymi EDR, NDR, GRC. Dostarczane rozwiązanie musi być systemem klasy SIEM (Security Information and Event Management z funkcjonalnością EDR (Endpoint Detection and Response) zapewniającym monitorowanie urządzeń końcowych (stacje robocze, serwery, drukarki itp.) i NDR (Network Detection and Response) zapewniającym monitorowanie urządzeń sieciowych, którego głównymi funkcjami są gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Korelacja zdarzeń polega na automatycznym, bieżącym wyszukiwaniu zależności między różnymi zdarzeniami z wielu źródeł, agregacji i wzbogacaniu danych na podstawie zdefiniowanych reguł. System powinien być wyposażony w funkcjonalność GRC (Governance, Risk Management and Compliance) w celu zarządzania podatnościami, ryzykiem i utrzymaniem zgodności środowiska IT zgodnie z obowiązującymi regulacjami (krajowym systemie cyberbezpieczeństwa, KRI, NIS2).

1. Zakres prac

Zakres prac obejmuje:

- **Dostarczenie licencji** na system SIEM.
- **Dostawa i instalacja środowiska serwerowego (fizycznego i wirtualnego)** niezbędnego do realizacji wdrożenia.
- **Instalacja i konfiguracja** systemu.
- **Integracja z infrastrukturą IT** urzędu:
 - 53 szt. komputerów PC
 - 5 szt. serwerów fizycznych (3 obecne + 2 nowe)
 - 8 szt. serwerów wirtualnych (8 obecne)
 - 2 szt. macierzy NAS
 - 1 szt. UTM

- Antywirus (ESET)
- 7 szt. przełączniki zarządzalne (nowe)
- Drukarki sieciowe
- Aplikacja kopii zapasowych
- Aplikacja zarządzania stacjami roboczymi
- System pocztowy
- **Dostosowanie reguł bezpieczeństwa** do specyfiki instytucji (ustalenie zakresu monitorowanych zdarzeń, dostosowanie alertów, itd.).
- **Implementacja 20 scenariuszy korelacji.**
- **Szkolenie personelu IT** z zakresu obsługi systemu SIEM, EDR, GRC.
- **Wsparcie techniczne i konserwacja** systemu przez okres 12 miesięcy po wdrożeniu.
- **Gwarancja:** 12 miesięcy

2. Wymagania funkcjonalne modułu SIEM

System SIEM powinien posiadać następujące funkcje:

- **Zbieranie i agregacja danych** z różnych źródeł w infrastrukturze IT, w tym logów z serwerów, urządzeń sieciowych, systemów operacyjnych, baz danych, aplikacji oraz systemów bezpieczeństwa.
- **Analiza zdarzeń** pod kątem bezpieczeństwa w czasie rzeczywistym.
- **Korelacja zdarzeń**, umożliwiająca identyfikację zagrożeń, które wynikają z pozornie niezwiązanych incydentów.
- **Automatyczne generowanie alarmów** w przypadku wykrycia zagrożeń.
- **Raportowanie** zgodne z wymaganiami Urzędu (miesięczne, kwartalne, ad-hoc).
- **Integracja z istniejącymi systemami bezpieczeństwa** (antywirus, firewall).
- **Panel zarządzania (dashboard)** z intuicyjnym interfejsem dla administratorów.
- System musi posiadać centralną konsolę zarządzania, umożliwiającą:
 - Real-time monitoring wszystkich agentów i komponentów systemu.
 - Zdalną konfigurację i aktualizację agentów.
 - Personalizację interfejsu dla różnych ról użytkowników."
- System musi umożliwiać:
 - Konfigurację reguł alertów.
 - Integrację z różnymi kanałami powiadomień (e-mail, SMS, komunikatory).
 - Definiowanie eskalacji incydentów i automatycznych reakcji."
- **Zgodność z przepisami prawa** dotyczącymi ochrony danych (RODO, ustawa o ochronie danych osobowych).

3. Wymagania techniczne modułu SIEM

- **Skalowalność:** System musi być skalowalny i zdolny do obsługi co najmniej 200 urządzeń końcowych i urządzeń sieciowych bez utraty wydajności. Powinien mieć możliwość rozbudowy w przyszłości w celu obsługi większej liczby źródeł logów i zdarzeń.

- **Wymagania sprzętowe:** Wykonawca dostarczy zasoby serwerowe w konfiguracji umożliwiającej realizację przedmiotu zamówienia.
- **Kompatybilność:** Dostarczone rozwiązanie powinno być kompatybilne z następującymi systemami operacyjnymi dla instalowanych agentów:
 - Windows: wersje desktopowe (7, 8.1, 10, 11) oraz serwerowe (Server 2012, 2016, 2019, 2022).
 - Linux: dystrybucje takie jak Ubuntu, Debian, CentOS, Red Hat Enterprise Linux, Oracle Linux.
 - macOS: wersje od Sierra (10.12) i nowsze.
- **Architektura agregacji** danych powinna umożliwiać rozwiązania z udziałem agentów oraz metody bezagentowe tam, gdzie instalacja agenta nie jest możliwa. System musi zbierać logi i zdarzenia z różnorodnych źródeł, w tym:
 - Serwery i stacje robocze (poprzez zainstalowanych agentów).
 - Urządzenia sieciowe NDR (routery, switchy, firewalles) za pomocą metod bezagentowych (np. Syslog).
 - Aplikacje i bazy danych.
 - Systemy bezpieczeństwa (np. NIDS/IPS).
 - Obsługa protokołów zbierania danych, takich jak Syslog, journald, integracje z PowerShell oraz RESTful API.
- **Baza danych** systemu SIEM/EDR musi wykorzystywać natywną i transparentną kompresję w otwartym standardzie, ze stopniem kompresji pozwalającym na uzyskanie co najmniej 3-krotnego zmniejszenia wolumenu danych na dysku w realnym użyciu.
- System musi zapewniać normalizację i korelację danych, automatycznie agregując zebrane informacje do jednolitego formatu.
- Administratorzy systemu muszą mieć możliwość definiowania własnych reguł detekcji i akcji responsywnych, z użyciem indywidualnych skryptów i interfejsów graficznych.
- System musi umożliwiać konfigurację interaktywnych pulpitów nawigacyjnych z możliwością personalizacji wizualizacji tabel, wykresów i statystyk oraz generowania raportów do ich dalszego eksportu.
- Rozwiązanie musi oferować zaawansowane mechanizmy detekcji zagrożeń, w tym:
 - Wykrywanie rootkitów i malware.
 - Monitorowanie integralności plików (FIM).
 - Analizę behawioralną systemu i aplikacji."

4. Wymagania dotyczące bezpieczeństwa modułu SIEM

- System powinien być zabezpieczony przed nieautoryzowanym dostępem.
- Dane zebrane przez SIEM muszą być przechowywane w sposób zabezpieczony, zgodny z polityką bezpieczeństwa Urzędu.
- Wdrożenie systemu nie może wymagać istotnych zmian w istniejącej infrastrukturze sieciowej Zamawiającego; wymagane są jedynie minimalne konfiguracje niezbędne do integracji.

- System powinien umożliwiać szyfrowanie komunikacji między komponentami.
- Rozwiązanie musi wspierać zgodność z międzynarodowymi standardami i regulacjami bezpieczeństwa, takimi jak GDPR, PCI DSS, HIPAA, oraz umożliwiać generowanie raportów zgodności.
- System musi umożliwiać integrację z istniejącymi narzędziami i usługami, takimi jak LDAP/Active Directory dla uwierzytelniania użytkowników, oraz wspierać Single Sign-On (SSO).

5. Wymagania modułu GRC Infrastruktura

- Aplikacja jest hostowana w infrastrukturze chmury publicznej wiodącego globalnego dostawcy, który jest wymieniony w najnowszej dostępnej wersji rankingu Gartner Magic Quadrant for Strategic Cloud Platform Services
- Baza danych jest hostowana w infrastrukturze chmury publicznej wiodącego globalnego dostawcy, który jest wymieniony w najnowszej dostępnej wersji rankingu Gartner Magic Quadrant for Strategic Cloud Platform Services
- Adres IP Interfejsu aplikacji znajduje się w klasie adresowej przypisanej do wiodącego globalnego dostawcy, który jest wymieniony w najnowszej dostępnej wersji rankingu Gartner Magic Quadrant for Strategic Cloud Platform Services oraz znajduje się na terenie EU
- Interfejs aplikacji jest dostępny tylko i wyłącznie w sieci lokalnej zamawiającego. Identyfikacja sieci zamawiającego jest realizowana za pomocą publicznego adresu IP bramy Zamawiającego. Interfejs aplikacji jest dostępny dla wskazanych przez zamawiającego hostów poza siecią zamawiającego za pomocą dedykowanych połączenie VPN. Ilość hostów tego typu nie będzie większa niż 10.
- Baza danych systemu jest automatycznie aktualizowana w zakresie poprawek bezpieczeństwa przez dostawcę chmury publicznej niezależnie od Zamawiającego i niezależnie od Wykonawcy.
- Serwer aplikacji jest automatycznie aktualizowany w zakresie poprawek bezpieczeństwa przez dostawcę chmury publicznej.
- Interfejs aplikacji jest dostępny na domenie TLD zamawiającego oraz certyfikatach TLS zamawiającego. Zamawiający przekierują adres domenowy na publiczny adres Wykonawcy w chmurze publicznej
- Ruch pomiędzy hostami zamawiającego a serwerem aplikacji jest zabezpieczony komunikacją szyfrowaną TLS w wersji 1.3. Na wyraźne życzenie Zamawiającego Wykonawca może wspierać dodatkowo komunikację TLS w wersji 1.2.
- Wykonawca odkłada kopię bezpieczeństwa bazy danych Zamawiającego w niezależnej infrastrukturze.

6. Wymagania modułu GRC Help Desk z bazą wiedzy

- Zarządzanie zgłoszeniami
System musi umożliwiać centralne zarządzanie zgłoszeniami użytkowników (tzw. "ticketami"), które mogą być tworzone automatycznie lub ręcznie przez klientów lub

pracowników. Zgłoszenia powinny obejmować takie informacje, jak opis problemu, priorytet, status, oraz przydzielony personel odpowiedzialny za rozwiązanie.

- Wielokanałowe wsparcie

System musi wspierać zbieranie zgłoszeń z różnych kanałów komunikacji, takich jak e-mail, formularze internetowe, czat na żywo. Każdy kanał powinien być zintegrowany z systemem, a zgłoszenia pochodzące z różnych źródeł muszą być przekształcane w tickety.

- Automatyzacja procesów

System musi wspierać automatyzację procesów obsługi zgłoszeń, w tym automatyczne przydzielanie zgłoszeń do odpowiednich działów lub pracowników na podstawie określonych reguł, takich jak priorytet, temat, czy źródło zgłoszenia. Automatyzacja powinna również obejmować powiadomienia dla klientów oraz pracowników w trakcie zmiany statusu zgłoszenia."

- Obsługa zgłoszeń według priorytetów i SLA

System musi pozwalać na przypisywanie priorytetów do zgłoszeń oraz definiowanie poziomów usług (SLA – Service Level Agreement) dla różnych typów zgłoszeń. Powinien umożliwiać śledzenie czasu reakcji oraz rozwiązania zgłoszeń w odniesieniu do ustalonych SLA, z możliwością generowania raportów dotyczących zgodności z SLA."

- Śledzenie historii i korespondencji

System musi umożliwiać pełne śledzenie historii każdego zgłoszenia, w tym korespondencji między użytkownikami a obsługą, załączników, komentarzy oraz wszelkich zmian statusu. Historia powinna być łatwo dostępna dla pracowników, co pozwala na szybkie odnalezienie poprzednich interakcji i rozwiązań.

- Baza wiedzy i wsparcie samoobsługowe

System musi oferować funkcjonalność bazy wiedzy, która pozwala na tworzenie artykułów i dokumentacji dostępnych dla klientów w celu samodzielnego rozwiązywania problemów. Baza wiedzy powinna być zintegrowana z systemem zgłoszeń poprzez możliwość przeszukiwania w jednym interfejsie użytkownika wraz ze zgłoszeniami.

- Raportowanie i analiza

System musi zapewniać rozbudowane funkcje raportowania, pozwalające na generowanie raportów dotyczących liczby zgłoszeń, czasu ich obsługi, zgodności z SLA, oraz efektywności zespołu.

- Zarządzanie użytkownikami i uprawnieniami

System musi umożliwiać definiowanie ról użytkowników oraz przypisywanie odpowiednich uprawnień w zależności od ich funkcji. Powinno być możliwe rozróżnienie poziomów dostępu, np. administratorów, pracowników obsługi i klientów, z możliwością konfiguracji uprawnień do tworzenia, przeglądania i edytowania zgłoszeń.

- Powiadomienia i eskalacje

System musi wspierać konfigurację automatycznych powiadomień i eskalacji w przypadku zgłoszeń, które wymagają natychmiastowej uwagi lub przekroczyły ustalone terminy SLA. Powiadomienia muszą być dostarczane za pomocą e-maila, SMS-a lub innych kanałów komunikacyjnych w zależności od preferencji użytkowników.

- Integracja z wieloma adresami e-mail dla poczty przychodzącej
System musi umożliwiać integrację z wieloma adresami e-mail dla poczty przychodzącej, co pozwala na automatyczne tworzenie zgłoszeń w oparciu o e-maile wysyłane na różne skrzynki pocztowe. Każdy adres e-mail może być powiązany z innym działem, projektem lub kategorią zgłoszeń, co umożliwia automatyczne kategoryzowanie i przydzielanie zgłoszeń do odpowiednich zespołów.
System musi umożliwiać wysyłkę automatycznych i manualnych wiadomości e-mail w odpowiedzi na zgłoszenia, z możliwością personalizacji treści e-maili. Automatyczne e-maile muszą być wysyłane w odpowiedzi na określone akcje, takie jak zmiana statusu zgłoszenia, aktualizacje w zgłoszeniu, przydzielenie zgłoszenia pracownikowi lub zamknięcie zgłoszenia. Wiadomości muszą zawierać szczegóły zgłoszenia oraz być dostosowane do brandingu firmy, z możliwością konfiguracji szablonów e-maili. System powinien także wspierać możliwość odpowiadania na zgłoszenia bezpośrednio z poziomu e-maila, co będzie automatycznie aktualizować ticket.
- Wyszukiwanie pełnotekstowe i filtrowanie zgłoszeń
System powinien umożliwiać zaawansowane wyszukiwanie pełnotekstowe oraz filtrowanie zgłoszeń według różnych kryteriów, co ułatwia zarządzanie dużą ilością zgłoszeń.
- Śledzenie czasu pracy i raportowanie czasu
System powinien umożliwiać śledzenie czasu pracy poświęconego na obsługę zgłoszeń oraz generowanie raportów czasu pracy dla celów rozliczeniowych lub analitycznych.
- System powinien umożliwiać:
Tworzenie predefiniowanych filtrów (widoków) zgłoszeń na podstawie kryteriów takich jak:
 - Adres e-mail, na który przyszło zgłoszenie (adres odbiorcy).
 - Adres e-mail, z którego przyszło zgłoszenie (adres nadawcy), co może wskazywać na konkretny dział.
 - Inne kryteria według potrzeb organizacji.
 - Przypisywanie widoczności tych filtrów do różnych grup agentów za pomocą uprawnień, tak aby:
 - Agenci obsługujący jeden dział w organizacji nie widzieli zgłoszeń z innego działu.
 - Inna grupa agentów (np. menedżerowie) mogła widzieć wszystkie zgłoszenia niezależnie od działu."

7. Wymagania modułu GRC Ryzyka

- Identyfikacja ryzyk

Moduł musi umożliwiać identyfikację ryzyk związanych z bezpieczeństwem informacji, zgodnie z wymaganiami normy ISO 27001 lub równoważne. Użytkownicy powinni mieć możliwość rejestrowania ryzyk związanych z zasobami IT, procesami, systemami i operacjami, z określeniem potencjalnych zagrożeń, podatności oraz skutków.

- Ocena i analiza ryzyka

Moduł musi wspierać przeprowadzanie oceny ryzyka zgodnie z ISO 27001 lub równoważne, uwzględniając prawdopodobieństwo wystąpienia ryzyka oraz jego potencjalne konsekwencje. Powinna być dostępna funkcjonalność oceny ryzyka zarówno jakościowej, jak i ilościowej.

- Zarządzanie ryzykiem i planowanie działań

Moduł musi umożliwiać definiowanie działań minimalizujących ryzyko, w tym wdrażanie kontroli, które mogą ograniczać lub eliminować ryzyka. System musi wspierać przypisywanie działań do konkretnych osób lub zespołów, z możliwością śledzenia postępów w realizacji planów redukcji ryzyka oraz dokumentowania wprowadzanych kontroli.

- Monitorowanie i przegląd ryzyka

Moduł musi zapewniać regularne monitorowanie ryzyk i efektywności wprowadzonych działań zapobiegawczych. Powinien umożliwiać okresowe przeglądy i aktualizacje ocen ryzyka, z możliwością rejestracji zmian.

- Rejestr ryzyk

Moduł musi zawierać centralny rejestr ryzyk, który przechowuje szczegółowe informacje o wszystkich zidentyfikowanych ryzykach, ich statusie, podjętych działaniach oraz odpowiedzialnych osobach. Rejestr musi być dostępny dla uprawnionych użytkowników, z możliwością filtrowania i wyszukiwania ryzyk według różnych kryteriów (np. kategoria ryzyka, poziom zagrożenia).

- Zgodność z ISO 27001 lub równoważne.

Moduł musi być zgodny z wymaganiami ISO 27001 lub równoważne dotyczącymi identyfikacji, oceny i zarządzania ryzykiem. Musi wspierać proces zgodny z załącznikiem A normy ISO 27001, umożliwiając śledzenie ryzyk w kontekście wdrażania odpowiednich środków kontroli i zgodności z politykami bezpieczeństwa organizacji.

- Raportowanie ryzyk i zgodności

System musi umożliwiać generowanie szczegółowych raportów dotyczących ryzyka, które mogą być dostosowywane do potrzeb organizacji. Raporty muszą obejmować analizę ryzyka, podjęte działania oraz poziom zgodności z wymaganiami ISO 27001 lub równoważne. Powinny być dostępne w różnych formatach (np. PDF, CSV).

- Zarządzanie uprawnieniami

System musi umożliwiać przypisywanie odpowiednich uprawnień do zarządzania ryzykiem. Musi oferować funkcje ograniczania dostępu do poszczególnych elementów modułu, aby zapewnić, że tylko upoważnieni użytkownicy mogą przeglądać, oceniać i zarządzać ryzykami.

8. Moduł Zarządzania Zgodnością

- Zarządzanie standardami
Moduł musi umożliwiać pracę na standardach takich jak ISO 27001 lub równoważne, pozwalając na zarządzanie elementami sterującymi i przypisanie ich do odpowiednich osób lub zespołów w organizacji.
- Tworzenie i zarządzanie SOA
System musi umożliwiać tworzenie i zarządzanie Oświadczeniem o Stosowalności (SOA), które przypisuje elementy sterujące do osób odpowiedzialnych za ich realizację wraz z uzasadnieniem stosowalności.
- Listy kontrolne zgodności
Moduł powinien umożliwiać tworzenie wskaźników zgodności oraz list zadań, które muszą być zrealizowane, aby spełnić wymagania poszczególnych elementów sterujących.
- Dodawanie materiałów dowodowych
System musi umożliwiać dodawanie materiałów dowodowych, w formie plików, które potwierdzają zgodność organizacji z wymaganiami norm.
- Audytowanie materiałów dowodowych
Moduł powinien wspierać audyt materiałów dowodowych na podstawie zdefiniowanych kryteriów akceptacji, aby zapewnić ich poprawność i zgodność z wymaganiami.
- Monitorowanie realizacji zadań
System musi umożliwiać monitorowanie statusu realizacji przypisanych zadań związanych ze zgodnością.
- Monitorowanie terminów aktualizacji materiałów dowodowych
Moduł musi automatycznie monitorować terminy aktualizacji materiałów dowodowych.
- Raportowanie zgodności
System musi umożliwiać generowanie raportów dotyczących zgodności, postępu realizacji zadań, oraz aktualności materiałów dowodowych, dostosowanych do potrzeb organizacji.
- Zgodność z ISO 27001 lub równoważne
Moduł musi być zgodny z wymaganiami normy ISO 27001 lub równoważne, w szczególności w zakresie zarządzania elementami sterującymi, materiałami dowodowymi i audytowania zgodności.
- Integracja z innymi modułami
System powinien być zintegrowany z innymi modułami GRC, takimi jak zarządzanie ryzykiem, w celu zapewnienia pełnej zgodności w organizacji.

9. Szkolenie i wsparcie techniczne

- Dostawca zobowiązuje się do przeprowadzenia szkolenia dla personelu IT z zakresu obsługi i administracji systemu dla 2 osób.

- Wsparcie techniczne obejmuje: telefoniczne, e-mailowe, zdalne wsparcie w rozwiązywaniu problemów związanych z działaniem systemu.