Załącznik nr 1b do SWZ
Znak 01/GK/08/26

Opis przedmiotu zamówienia – część II

na usługę pn.:

„Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z realizacja szkoleń z zakresu cyberbezpieczeństwa" w ramach projektu pn. „Cyberbezpieczne Wodociągi Miejskie Sp. z o.o. w Braniewie" finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) Priorytet: C3 Cyberbezpieczeństwo, Działanie C3.1.1. Cyberbezpieczeństwo - CyberPL, konkurs grantowy pn. "Cyberbezpieczne Wodociągi" o numerze KPOD.05.10-CW.01-001/25

Braniewo, dnia: 18.08.2026 r.

Zatwierdza:
Prezes Zarządu

Szczegółowy zakres

Przedmiot zamówienia został podzielony na następujące elementy i obejmuje w szczególności:

1. Doskonalenie SZBI (1.1.3)

1. Wykonawca jest zobowiązany do przeglądu i dostosowania wdrożonego u Zamawiającego SZBI, obejmującego polityki, procedury, instrukcje mające na celu zarządzanie ryzykiem związanym z bezpieczeństwem informacji, do aktualnych wymagań prawnych powiązanych z cyberbezpieczeństwem
2. SZBI musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT. Zaktualizowane musi zostać również szacowanie ryzyka (na podstawie ISO/IEC 27005), obejmujące inwentaryzację aktywów, identyfikację zagrożeń i podatności, ocenę prawdopodobieństwa i skutków oraz opracowanie planu postępowania z ryzykiem.
3. Przeglądu i doskonalenia SZBI należy dokonać w następujących obszarach:

a) ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych, w tym polityk analizy ryzyka i bezpieczeństwa systemów informatycznych;
b) aktualizacje regulacji wewnętrznych w zakresie bezpieczeństwa informacji;
c) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
d) opracowanie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
e) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji;
f) bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami;
g) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia;
h) zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji, w tym przeprowadzanie szkoleń w zakresie cyberbezpieczeństwa;
i) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
j) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
k) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionym osobom jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
l) opracowanie polityk i procedur stosowania kryptografii;
m) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między Zamawiającym, a jego bezpośrednimi dostawcami, usługodawcami i poddostawcami;
n) zawierania w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
o) ciągłość działania kluczowych usług, w tym zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej oraz zarządzanie kryzysowe;

p) stosowanie uwierzytelniania wieloskładnikowego oraz ciągłych, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych;
q) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w tym bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych oraz postępowanie w przypadku wykrycia podatności i ich ujawnianie;
r) zarządzanie incydentami bezpieczeństwa informacji i cyberbezpieczeństwa;
s) zapewnienia okresowego audytu cyberbezpieczeństwa;

4. Doskonalenie SZBI musi obejmować bezpieczeństwo fizyczne (ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwo informatyczne (bezpieczeństwo systemu teleinformatycznego) oraz bezpieczeństwo osobowe i organizacyjne (stosowane procedury bezpieczeństwa).
5. Udoskonalone SZBI musi uwzględniać wymagania następujących aktów prawnych oraz norm:

a) Norma PN-EN ISO/IEC 27001:2023;
b) Norma PN-EN ISO/IEC 27002:2023;
c) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
d) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

6. Wykonawca ma obowiązek przekazać Zamawiającemu:

- dostosowaną do aktualnych wymagań prawnych dokumentację systemu zarządzania bezpieczeństwem informacji;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

7. Wykonawca zapewni bieżące wsparcie merytoryczne dla zespołu wdrożeniowego w trakcie całego procesu doskonalenia systemu. Konsultacje będą odbywać się w dni robocze, od poniedziałku do piątku, za pośrednictwem bezpiecznych kanałów komunikacji, takich jak rozmowy telefoniczne, korespondencja e-mailowa, telekonferencje lub bezpośrednie spotkania w siedzibie Zamawiającego.

2. Doradztwo (1.1.13)

1. Przedmiotem zamówienia jest świadczenie usługi doradztwa w zakresie opracowania warunków umów kontraktowych na wdrożenie i utrzymanie infrastruktury w zakresie cyberbezpieczeństwa, obejmujących m.in. łańcuch dostaw, infrastrukturę monitorowania i zarządzania oraz usługi zdalne, w środowiskach IT/OT/ICS/IIoT.
2. Zakres doradztwa obejmuje w szczególności:
a) opracowanie i weryfikację wzorcowych postanowień umownych (warunków kontraktowych) dotyczących nabywania, wdrażania oraz utrzymania rozwiązań i infrastruktury cyberbezpieczeństwa;

b) uwzględnienie wymagań bezpieczeństwa łańcucha dostaw, w tym relacji Zamawiającego z dostawcami, usługodawcami i poddostawcami;
c) postanowienia dotyczące infrastruktury monitorowania i zarządzania bezpieczeństwem oraz świadczenia usług zdalnych (m.in. zdalny dostęp serwisowy, utrzymanie, aktualizacje);
d) uwzględnienie specyfiki środowisk IT/OT/ICS/IIoT, w tym wymagań w zakresie ciągłości działania oraz segmentacji i bezpieczeństwa systemów sterowania;
e) rekomendacje dotyczące poziomów świadczenia usług (SLA), wymagań gwarancyjnych i serwisowych oraz klauzul bezpieczeństwa informacji.
3. Doradztwo stanowi element utrzymania, zarządzania i doskonalenia SZBI, obejmujący bieżące wsparcie w zakresie procedur i warunków kontraktowych, co jest niezbędne dla trwałości efektów projektu.
4. Usługa doradztwa świadczona będzie w sposób ciągły przez okres do 7 miesięcy, nie dłużej niż do upływu terminu realizacji zamówienia określonego w SWZ. Konsultacje odbywać się będą w dni robocze, za pośrednictwem bezpiecznych kanałów komunikacji (rozmowy telefoniczne, korespondencja e-mail, telekonferencje lub bezpośrednie spotkania w siedzibie Zamawiającego).

3. Szkolenie podstawowe dla pracowników (2.1.1) (15 osób)

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.
Szkolenie musi być zrealizowane w siedzibie Zamawiającego.

W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni.

Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny. Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem. Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację.

Szkolenie musi być skierowane do wytypowanego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne.
Korzyści po szkoleniu:

- zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi
- zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi

Wykonawca zobowiązany jest do:

- wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika,
- zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

Zakres merytoryczny szkolenia:

- Co to jest cyberprzestępczość?
- Opis funkcjonowania zorganizowanych grup cyberprzestępczych
- Czy jestem atrakcyjnym „klientem" dla cyberprzestępcy?
- Jakie zyski może mieć cyberprzestępca atakując moje dane?
- Straty wynikające z udanego ataku
- Rodzaje ataków skierowane w użytkowników Internetu
- Jak bronić się przed cyberprzestępcami?
- Spam jako niegroźny sposób na groźne ataki • Handel adresami e-mail
- Kampanie Phishingowe
- Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję
- Groźne ataki 0-day
- Nieopłacona FV jako sposób przemycenia wirusa do naszego komputera
- Ataki socjotechniczne - czyli niewinne „wyłudzanie" danych
- Przekazywanie haseł dostępowych znajomym
- Fizyczne bezpieczeństwo danych osobowych
- Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy
- Aktualne zagrożenia wynikające z wojny w Ukrainie
- Podsumowanie szkolenia, pytania, dyskusja

4. Szkolenie ogólne dla kadry i informatyków (2.1.3) (10 osób)

Przedmiotem zamówienia jest przeprowadzenie szkoleń dla informatyków i kadry zarządzającej z zakresu cyberbezpieczeństwa

Wymagania dla szkoleń dla informatyków i kadry zarządzającej:

a) Szkolenia muszą być zrealizowane w siedzibie Zamawiającego.
b) W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trener muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny.
c) Minimalny zakres tematyczny:

Szkolenie dla kadry zarządzającej z zakresu cyberbezpieczeństwa:

- Wstęp do bezpieczeństwa w cyberprzestrzenii;
- Akty Prawne;
- Krajowy System Cyberbezpieczeństwa;
- Analiza ataków cybernetycznych;
- Najpopularniejsze zagrożenia;
- Przewodnik po metodach obrony instytucji;zapis
- Cyberbezpieczeństwo osobiste;

- Postępowanie w pracy;
- ABC higieny pracy w cyberprzestrzeni;
- Bezpieczeństwo pracy zdalnej;
- Ataki socjotechniczne - czyli niewinne „wyłudzanie" danych;
- Kampanie Phishingowe;
- Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję;
- Aktualne zagrożenia wynikające z wojny w Ukrainie;
- Dyskusja.

Szkolenie dla informatyków z zakresu cyberbezpieczeństwa:

- Akty prawne dotyczące cyberbezpieczeństwa;
- Krajowy system Cyberbezpieczeństwa;
- Cyberbezpieczeństwo instytucjonalne;
- Analiza ataku cybernetycznego;
- Metody obrony przed cyberzagrożeniami;
- Zasady bezpiecznej konfiguracji sprzętu;
- Metody utwardzania urządzeń i systemów;
- Cyberbezpieczeństwo osobiste;
- Podstawy kryptografii;
- Ataki socjotechniczne;
- Dyskusja.

1. Wykonawca zobowiązany jest do:

a) wydania imiennych certyfikatów dla każdego uczestnika,
a) zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

5. Szkolenie Wazuh (lub równoważne) dla informatyków zespołu IT i OT (2.1.3) (5 osób)

Przedmiot zamówienia
Wykonawca zapewni realizację na rzecz Zamawiającego **5 indywidualnych szkoleń** z zakresu instalacji, konfiguracji i eksploatacji systemu klasy SIEM (Security Information and Event Management) opartego o oprogramowanie Wazuh, dla uczestników wskazanych przez Zamawiającego.

2. Sposób realizacji szkolenia
Szkolenia mogą być realizowane:

- w terminach otwartych ogłaszanych przez Wykonawcę, albo

- w terminie indywidualnie uzgodnionym z Zamawiającym, jeżeli w danym okresie nie będzie dostępnego terminu otwartego odpowiadającego potrzebom Zamawiającego.

Wykonawca zapewni, aby każde szkolenie zostało przeprowadzone przez osobę lub podmiot posiadający odpowiednie kompetencje merytoryczne i praktyczne w zakresie przedmiotu szkolenia.

3. Certyfikacja uczestników

Każde szkolenie zakończy się wydaniem uczestnikowi **certyfikatu ukończenia szkolenia** albo równoważnego dokumentu potwierdzającego udział i nabycie kompetencji, zgodnie ze standardem stosowanym przez centrum szkoleniowe lub Wykonawcę, pod warunkiem że dokument ten będzie potwierdzał odbycie szkolenia z zakresu wskazanego w OPZ.

4. Termin realizacji

Wykonawca zapewni realizację szkolenia w terminie nie dłuższym niż ramy realizacji projektu czyli do 30.11.2026.

5. Odpowiedzialność Wykonawcy

W przypadku powierzenia realizacji szkolenia podwykonawcy lub centrum szkoleniowemu, Wykonawca pozostaje odpowiedzialny wobec Zamawiającego za należyte wykonanie całości usługi, w tym za terminowość, zgodność programu szkolenia z OPZ

3. Forma realizacji szkolenia

- Forma szkolenia: zdalna (online), prowadzona na żywo przez trenera w czasie rzeczywistym, z możliwością bieżącej interakcji uczestnika z prowadzącym (zadawanie pytań, dyskusja).
- Łączny czas trwania szkolenia: minimum 14 godzin zegarowych.
- Język szkolenia: język polski.

4. Zakres merytoryczny szkolenia

Program szkolenia musi obejmować minimum następujące obszary tematyczne. Kolejność oraz szczegółowy podział na sesje/dni szkoleniowe pozostają w gestii Wykonawcy. Zamawiający dopuszcza szkolenie równoważne z systemu Wazuh

4.1. Instalacja i podstawy konfiguracji Wazuh

- Wprowadzenie do Wazuh: funkcje, zastosowania i miejsce SIEM w bezpieczeństwie IT.
- Szczegółowa architektura: rola serwera, agentów, indexera oraz interfejsu graficznego.
- Pobranie i instalacja serwera Wazuh w środowisku Linux
- Konfiguracja agentów na systemach Windows i Linux; w tym tryb agentless na urządzeniach sieciowych (Syslog).
- Testowanie komunikacji między agentami i serwerem, podstawowy tuning ustawień.
- Wprowadzenie do zarządzania dashboardem Wazuh i monitorowanie pierwszych zdarzeń.

4.2. Zaawansowana konfiguracja i monitorowanie

- Tworzenie i modyfikacja reguł detekcji, pisanie własnych dekoderów do logów niestandardowych.
- Ustawienia monitorowania integralności plików (FIM) oraz detekcja rootkitów.
- Przegląd i rozszerzenie polityk bezpieczeństwa, konfiguracja alertów i powiadomień.
- Automatyzacja reakcji na incydenty (Active Response) i integracja z narzędziami IDS/IPS.

- Analiza logów oraz optymalizacja wydajności systemu poprzez tuning indeksów i konfiguracji indexera.
- Tworzenie i dostosowywanie dashboardów zgodnie z potrzebami codziennego monitoringu i raportowania.

6. Szkolenie Zabbix (lub równoważne) dla informatyków zespołu IT i OT (2.1.3) (5 osób)

1. Przedmiot zamówienia

Wykonawca zapewni realizację na rzecz Zamawiającego **5 indywidualnych szkoleń** z zakresu konfiguracji, administracji i utrzymania systemu monitoringu infrastruktury IT opartego o oprogramowanie Zabbix (lub równoważne), dla uczestników wskazanych przez Zamawiającego.

Szkolenia zostaną zrealizowane przez Wykonawcę albo przez podmiot trzeci działający w charakterze podwykonawcy lub centrum szkoleniowego posiadające odpowiednie kompetencje, doświadczenie oraz zaplecze techniczne do przeprowadzenia szkolenia zgodnie z wymaganiami niniejszego OPZ.

2. Sposób realizacji szkolenia

Szkolenia mogą być realizowane:

- w terminach otwartych ogłaszanych przez Wykonawcę, albo
- w terminie indywidualnie uzgodnionym z Zamawiającym, jeżeli w danym okresie nie będzie dostępnego terminu otwartego odpowiadającego potrzebom Zamawiającego.

Wykonawca zapewni, aby każde szkolenie zostało przeprowadzone przez osobę lub podmiot posiadający odpowiednie kompetencje merytoryczne i praktyczne w zakresie przedmiotu szkolenia

3. Termin realizacji

Wykonawca zapewni realizację szkolenia w terminie nie dłuższym niż ramy realizacji projektu, tj. do **30.11.2026 r.**

4. Odpowiedzialność Wykonawcy

W przypadku powierzenia realizacji szkolenia podwykonawcy lub centrum szkoleniowemu, Wykonawca pozostaje odpowiedzialny wobec Zamawiającego za należyte wykonanie całości usługi, w tym za terminowość oraz zgodność programu szkolenia z OPZ.

5. Forma realizacji szkolenia

- Forma szkolenia: zdalne (online), prowadzone na żywo przez trenera w czasie rzeczywistym, z możliwością bieżącej interakcji uczestnika z prowadzącym (zadawanie pytań, dyskusja).
- Łączny czas trwania szkolenia: minimum 20 godzin zegarowych.
- Język szkolenia: język polski.

6. Zakres merytoryczny szkolenia

Program szkolenia musi obejmować minimum następujące obszary tematyczne. Kolejność oraz szczegółowy podział na sesje pozostają w gestii Wykonawcy.

6.1. Architektura i instalacja systemu

- Rola systemu monitoringu w infrastrukturze IT oraz przegląd możliwości oprogramowania Zabbix.
- Komponenty systemu i ich rola: serwer monitoringu, baza danych, interfejs webowy (frontend), agent, proxy - przepływ danych pomiędzy komponentami.
- Wersje oprogramowania i wymagania środowiskowe.
- Instalacja serwera wraz z bazą danych oraz uruchomienie interfejsu webowego.
- Konfiguracja początkowa (konto administracyjne, strefa czasowa, lokalizacja, układ interfejsu).

6.2. Konfiguracja hostów, agentów i elementów monitorowanych

- Instalacja i konfiguracja agenta monitoringu w systemach Linux oraz Microsoft Windows.
- Dodawanie hostów: nazwy, grupy, interfejsy komunikacyjne.
- Tryby pracy agenta: pasywny i aktywny - różnice, zastosowania, przypadki użycia.
- Elementy danych (items): typy, klucze, interwały i okresy pobierania, historia, jednostki.
- Wykorzystanie szablonów wbudowanych dla najpopularniejszych systemów operacyjnych.
- Wizualizacja danych w widoku bieżących wartości oraz proste wykresy.
- Diagnostyka problemów komunikacji agent-serwer.

6.3. Reguły, akcje i powiadomienia

- Triggery (reguły wyzwalania alarmów): zasada działania, składnia, przykłady (CPU, dysk, pamięć).
- Mechanizmy histerezy, funkcje czasowe, sposoby zapobiegania efektowi flappingu.
- Poziomy istotności (severity) zdarzeń.
- Akcje (actions): warunki wyzwalania, operacje, odbiorcy.
- Typy mediów (media types): konfiguracja powiadomień przez e-mail, SMS oraz webhook.
- Mechanizmy potwierdzania zdarzeń (acknowledge) oraz trybu konserwacji (maintenance).
- Komendy zdalne (remediation) - podstawy.

6.4. Szablony, makra i automatyczne wykrywanie (LLD)

- Koncepcja szablonów (templates) i ponowne wykorzystanie konfiguracji.
- Przypisywanie wielu szablonów do pojedynczego hosta.

- Tworzenie własnych szablonów dla aplikacji i usług.
- Makra: zakres globalny, szablonowy, hostowy - mechanizm nadpisywania.
- Parametryzacja progów reguł przy użyciu makr.
- Low-Level Discovery: automatyczne wykrywanie systemów plików, interfejsów sieciowych, usług.
- Prototypy elementów danych i reguł w mechanizmie LLD.
- Eksport i import szablonów w formatach XML / YAML / JSON.

6.5. Wizualizacja danych i skalowanie środowiska

- Tworzenie dashboardów i konfiguracja widgetów.
- Wykresy oraz mapy sieciowe.
- Widoki operacyjne dla zespołów utrzymaniowych.
- Raporty SLA i konfiguracja usług biznesowych (services).
- Zabbix Proxy: zastosowanie w środowiskach rozproszonych, korzyści, ograniczenia.
- Instalacja, konfiguracja i monitorowanie pracy proxy.

6.6. API, automatyzacja i rozszerzanie funkcjonalności

- Interfejs programistyczny (API) typu JSON-RPC: endpoint, uwierzytelnianie, tokeny, podstawowe metody.
- Masowe operacje konfiguracyjne (np. zasilanie z systemów CMDB / plików CSV) z wykorzystaniem API.
- Tworzenie własnych metryk po stronie agenta (UserParameters).
- Mechanizm external checks po stronie serwera.
- Model push: trapper oraz narzędzie zabbix_sender.
- Skrypty mediów i webhooków - integracje z systemami zewnętrznymi.

6.7. Bezpieczeństwo i utrzymanie środowiska

- Role i uprawnienia użytkowników, zasada najmniejszych uprawnień.
- Dostępy do hostów, grup hostów i danych.
- Bezpieczeństwo API.
- Utwardzanie (hardening) interfejsu webowego, agentów i proxy - w tym szyfrowanie komunikacji.
- Monitorowanie samego systemu monitoringu.
- Aktualizacje, kopie zapasowe oraz skalowanie serwera w środowiskach produkcyjnych.

6.8. Praktyczne aspekty operacyjne

- Dobre praktyki w zakresie polityki alertowania.
- Definiowanie zależności pomiędzy zasobami w celu redukcji szumu alertowego.
- Tryby maintenance: planowany, awaryjny, per-host.
- Tagowanie zasobów i zdarzeń.

- Zarządzanie problemami i eskalacja do kolejnych linii wsparcia.
- Tworzenie i wykorzystanie runbooków.
- Pożądane jest omówienie możliwości integracji systemu monitoringu z zewnętrznymi narzędziami opartymi o sztuczną inteligencję (np. w celu redukcji liczby powtórnych alarmów lub analizy logów).

7. Materiały szkoleniowe i potwierdzenie ukończenia

W ramach realizacji szkolenia Wykonawca zapewni uczestnikowi minimum:

- Materiały szkoleniowe w formie elektronicznej (np. prezentacje, dokumentacja konfiguracyjna).
- Ćwiczenia praktyczne / laboratoryjne do samodzielnej realizacji.
- Imienny dokument potwierdzający ukończenie szkolenia (certyfikat lub zaświadczenie) w formie elektronicznej (PDF) - w języku polskim lub w wersji dwujęzycznej (polski / angielski).

Wymagania dotyczące zdolności technicznej oraz zawodowej – znajdują się w dokumencie SWZ - 17.1.5. - Zdolność techniczna lub zawodowa.

Signed by / Podpisano przez:

Bartłomiej Adam Fita

Date / Data: 2026-08-18 12:32