Załącznik nr 8 do SWZ – Opis przedmiotu zamówienia (OPZ)

Numer zamówienia: TZP/007/26

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa i wdrożenie rozwiązań z zakresu cyberbezpieczeństwa oraz świadczenie usług w zakresie bezpieczeństwa informacji i ciągłości działania" w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o."

Cztery powiązane i nierozerwalne zadania

Zamawiający: Miejskie Wodociągi i Kanalizacja w Kędzierzynie-Koźlu spółka z ograniczoną odpowiedzialnością

Dokument: Opis przedmiotu zamówienia

Data: 6 października 2026 r.

Spis treści

1 Przedmiot zamówienia i zasady realizacji ... 4
1.1 Podstawy wykonania ... 4
1.2 Bezpieczeństwo ludzi i procesów technologicznych ... 4
1.3 Ochrona informacji i dokumentacji ... 5
2 Kody CPV ... 6
3 Zależności i integracje czterech zadań ... 7
I01 SZBI i SZCD STI do GRC ... 7
I02 Systemy IT i dopuszczone źródła OT do SIEM ... 7
I03 IDS OT do SIEM ... 7
I04 SIEM do SOAR do SOC ... 7
I05 SOC i GRC do SZBI i SZCD STI ... 7
I06 Systemy zintegrowane do nadzoru SOC ... 8
4 Zadanie 1 Szkolenia oraz obszar kompetencyjny i organizacyjny wraz z SZBI ... 9
4.1 Przedmiot cel i zakres ... 9
4.2 Zakres rzeczowy i wymagania dotyczące realizacji zadania 1 ... 9
4.3 Etapy integracje i przekazanie wiedzy ... 25
4.4 Obowiązki stron bezpieczeństwo i odbiór ... 25
4.5 Zakończenie współpracy ... 26
5 Zadanie 2 System klasy SIEM/SOAR z modułem GRC ... 27
5.1 Przedmiot cel i zakres zamówienia ... 27
5.2 Wymagania funkcjonalne, techniczne i realizacyjne SIEM/SOAR z modułem GRC ... 27
5.3 Etapy realizacji i integracje ... 35
5.4 Obowiązki stron i bezpieczeństwo ... 35
5.5 Okres licencji i wsparcia ... 35
5.6 Testy i kryteria odbioru ... 35
5.7 Zakończenie współpracy ... 35
6 Zadanie 3 Wdrożenie IDS OT oraz dostawa jednej zapory bezpieczeństwa ... 36
6.1 Przedmiot cel i zakres ... 36
6.2 Wymagania funkcjonalne, techniczne i realizacyjne monitorowania OT ... 36
6.3 Etapy i integracje ... 38
6.4 Produkty dokumentacja i szkolenia ... 39
6.5 Obowiązki stron i ochrona procesu ... 39
6.6 Licencje gwarancja utrzymanie i serwis ... 39
6.7 Testy i kryteria odbioru ... 39
6.8 Zakończenie współpracy ... 39
7 Zadanie 4 Usługa monitoringu SOC dla środowisk IT i OT ... 40
7.1 Przedmiot cel i zakres ... 40
7.2 Wymagania dotyczące realizacji usługi SOC ... 40
7.3 Uruchomienie i integracje ... 41

7.4 Obsługa incydentów i pomiar czasów 41
7.5 Telemetria raportowanie i współpraca 41
7.6 Obowiązki bezpieczeństwo i wiedza 41
7.7 Produkty testy i kryteria odbioru 41
7.8 Zakończenie usługi 42
8 Odbiór całości i kontrola zależności 43
9 Słownik pojęć 44
Załącznik A. Dostawa i wdrożenie jednej zapory bezpieczeństwa 46
A.1 Przedmiot i zakres dostawy 46
A.2 Wymagania funkcjonalne, techniczne i realizacyjne 46
A.3 Integracja, ochrona danych i bezpieczeństwo wdrożenia 52
A.4 Produkty i kryteria odbioru 52
A.5 Rozmieszczenie i parametry wdrożenia 52

1 Przedmiot zamówienia i zasady realizacji

Przedmiotem zamówienia jest podniesienie poziomu cyberbezpieczeństwa środowisk IT i OT przedsiębiorstwa wodociągowego przez realizację czterech zadań: rozwój kompetencji i systemów zarządzania wraz z usługą Security Awareness; wdrożenie SIEM/SOAR z modułem GRC; dostawa i wdrożenie IDS OT oraz jednej zapory bezpieczeństwa do separacji IT/OT; monitoring SOC. Szczegółowe wymagania dla zapory zawiera załącznik A. Wykonawca zapewni spójność integracji, przepływu informacji, odpowiedzialności, dokumentacji i odbiorów całego zakresu.

Zadania tworzą nierozerwalną całość funkcjonalną: zasady organizacyjne wyznaczają sposób wykorzystania technologii, a wyniki detekcji i monitorowania służą aktualizacji ryzyka oraz doskonaleniu zasad. Wykonawca zapewni jednego koordynatora integracji i uzgodniony harmonogram zależności.

Godzina oznacza 60 minut pracy merytorycznej bez przerw. Dzień roboczy oznacza poniedziałek-piątek z wyłączeniem dni ustawowo wolnych od pracy w Polsce. Harmonogramy szczegółowe muszą mieścić się w terminach zamówienia.

Każde szkolenie przewidziane w OPZ, w tym produktowe, techniczne i administracyjne, zapewnia udział uczestników wskazanych przez Zamawiającego. Dopuszcza się podział na grupy; każdy uczestnik otrzymuje pełny program i cały wymagany wymiar godzin danego szkolenia. Organizacja wszystkich grup jest uwzględniona w cenie. Szkolenia pozostają w zadaniach, z których wynikają. Zasada ta nie zmienia liczebności spotkań, warsztatów ani ćwiczeń, które nie są szkoleniami.

1.1 Podstawy wykonania

Wykonawca zapewni identyfikację przepisów właściwych dla potwierdzonego statusu Zamawiającego, w tym ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa z późniejszymi zmianami, w tym zmianą z 23 stycznia 2026 r., oraz rozporządzenia (UE) 2016/679 w zakresie przetwarzania danych osobowych.

Punktem odniesienia metodycznego dla SZBI jest ISO/IEC 27001:2022 wraz z Amd 1:2024, dla SZCD STI ISO 22301:2019 wraz z Amd 1:2024, a dla ochrony OT NIST SP 800-82 Rev. 3. Dopuszcza się równoważną metodykę w zakresie wskazanym w zadaniu 1, przy wykazaniu pokrycia czynności, produktów i odbiorów. Normy i wytyczne nie są samoistnym obowiązkiem ustawowym. Zadanie 1 nie obejmuje certyfikacji systemów Zamawiającego. Wymagania certyfikacyjne Wykonawcy określa rozdział 2.

1.2 Bezpieczeństwo ludzi i procesów technologicznych

Wykonawca zapewni nadrzędność bezpieczeństwa ludzi, jakości i ciągłości dostaw wody oraz ochrony procesu technologicznego nad realizacją testów i zmian. Zamawiający zapewni wskazanie odrębnych właścicieli IT, OT i eksploatacji oraz osób uprawnionych do decyzji o działaniu i przywróceniu procesu.

Wykonawca zapewni wcześniejszą autoryzację prac oddziałujących na środowisko, uzgodnione okna, ocenę wpływu i plan wycofania. Zamawiający może natychmiast przerwać czynności. Wykonawca zapewni bezpieczne zatrzymanie prac i zapis przyczyny, wykonanych działań oraz warunków wznowienia.

Zakazane są nieuzgodnione próby destrukcyjne, nieautoryzowane sterowanie urządzeniami OT oraz aktywne skanowanie OT bez odrębnej autoryzacji. Wymaganie pasywnego IDS nie stanowi zezwolenia na aktywne testy. Funkcje blokowania, automatyzacji i zdalnej zmiany konfiguracji mogą być uruchamiane wyłącznie w zatwierdzonym zakresie.

Wykonawca zapewni stosowanie danych testowych lub zanonimizowanych, gdy pozwalają osiągnąć cel, bezpieczny dostęp zdalny, uprawnienia ograniczone do niezbędnego zakresu, ewidencję działań administracyjnych i możliwość odebrania dostępu. Ograniczenia techniczne uwierzytelniania wieloskładnikowego w OT wymagają zatwierdzonych środków kompensacyjnych.

Wykonawca zapewni niezwłoczne przekazanie informacji o krytycznym zagrożeniu uzgodnionym kanałem, bez oczekiwania na raport okresowy. Zamawiający zapewni kontakt podstawowy i awaryjny oraz uprawnionego odbiorcę powiadomień.

Wykonawca zapewni kontrolę podwykonawców i łańcucha dostaw, wykaz podmiotów mających dostęp do danych lub systemów oraz przeniesienie na nie właściwych obowiązków bezpieczeństwa. Wykonawca odpowiada za koordynację ich prac i zgłaszanie zmian wpływających na zakres lub ryzyko.

1.3 Ochrona informacji i dokumentacji

Wykonawca zapewni poufność informacji o architekturze, zabezpieczeniach, podatnościach, incydentach, warunkach umów i osobach. Dane wrażliwe przekazuje się wyłącznie uprawnionym odbiorcom zabezpieczonym kanałem. Publiczny opis skali środowiska musi umożliwiać porównywalną wycenę; szczegółowe inwentarze, adresacja i punkty przyłączenia są udostępniane w kontrolowanym trybie.

Wykonawca przekaże dokumentację w języku polskim, w postaci edytowalnej i PDF, z identyfikatorem, wersją, właścicielem i statusem zatwierdzenia. Zamawiający uzyska prawo wewnętrznego wykorzystania, aktualizacji oraz udostępnienia następnemu wykonawcy do utrzymania. Nie wymaga się przekazywania licencjonowanych tekstów norm. Prawa do oprogramowania i konfiguracji należy określić odrębnie w warunkach licencyjnych.

Wykonawca zapewni zwrot albo bezpieczne usunięcie danych roboczych, potwierdzenie wykonania oraz plan wycofania kont, kluczy i połączeń po zakończeniu prac. Dane podlegające uzasadnionej retencji pozostają chronione do jej końca. Dokumentację i dostępy przekazuje się uprawnionym osobom Zamawiającego przy zakończeniu prac, zabezpieczonym kanałem; dostęp Wykonawcy jest następnie odbierany. Przekazanie usługi SOC odbywa się zgodnie z 7.8.

2 Kody CPV

Główny kod CPV:

72222000-7 – Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej oraz usługi w zakresie planowania

Dodatkowe kody CPV:

48730000-4 – Pakiety oprogramowania zabezpieczającego

72260000-5 – Usługi w zakresie oprogramowania

32420000-3 – Urządzenia sieciowe

72250000-2 – Usługi w zakresie konserwacji i wsparcia systemów

80533100-0 – Usługi szkolenia komputerowego

72263000-6 – Usługi wdrażania oprogramowania

72268000-1 – Usługi dostawy oprogramowania

80510000-2 – Usługi szkolenia specjalistycznego

72224000-1 – Usługi doradcze w zakresie zarządzania projektem

79111000-5 – Usługi w zakresie doradztwa prawnego

72253000-3 – Usługi pomocy komputerowej i podobne

3 Zależności i integracje czterech zadań

Opis środowiska stanowiący podstawę OPZ

Środowisko Zamawiającego obejmuje cztery lokalizacje i 22 sieci VLAN, urządzenia routingu i przełączania oraz zaporę na brzegu Internetu. Szczegółowe lokalizacje, topologia i konfiguracje są udostępniane w kontrolowanym trybie zgodnie z 1.3.

Środowisko obejmuje trzy hosty wirtualizacji, serwer kopii zapasowych, usługę serwera zewnętrznego oraz pamięć masową NAS. Działa 12 systemów wirtualnych: trzy systemy SCADA, w tym archiwizacja i udostępnianie danych procesowych; trzy systemy ERP i obiegu dokumentów; dwa systemy GIS; dwa systemy pomocnicze oraz dwa systemy obsługi IT i dostępu zdalnego. Wykorzystywane są systemy Windows i Linux.

Inwentarz zawiera 53 komputery biurowe oraz 60 licencji ochrony stacji końcowych. Charakter źródeł SIEM obejmuje logi systemów operacyjnych i aplikacji, hostów wirtualizacji, urządzeń sieciowych, dostępu zdalnego, ochrony endpointów, kopii zapasowych oraz alerty IDS. Liczba pozycji inwentarza nie jest sposobem obliczania licencji SIEM; wymagane minimum określa pkt 3 rozdziału w 5.2.

Środowisko wykorzystuje kopie zapasowe serwerów, stacji roboczych i usług zewnętrznych, pamięć NAS, nośniki taśmowe oraz replikację maszyn wirtualnych. Dokumentacja i wyniki sprawdzeń odtworzenia stanowią dane wejściowe do prac nad ciągłością działania. Wykorzystywane są również usługi zdalnego dostępu i wsparcia.

Wymagania dotyczące możliwości integracji produktu z usługami katalogowymi lub chmurowymi nie oznaczają zamówienia wdrożenia takich usług. Integracje obejmują źródła w zakresie zadań 2-4.

Środowisko obejmuje istniejący monitoring OT. Zakres zamawianej dostawy nowych sond, komponentu zarządzającego i licencji określa 6.2; istniejące wyposażenie nie zastępuje tej dostawy.

W zadaniu 3 przewidziano dostawę jednej zapory do separacji sieci IT i OT, zgodnie z załącznikiem A. Zapora IT/OT i pasywny IDS pełnią odrębne funkcje.

Zadanie 1 dostarcza zasady, właścicieli i ryzyka do konfiguracji GRC w zadaniu 2. IDS w zadaniu 3 dostarcza telemetrię i alerty OT do SIEM, który łączy je z danymi IT. SOAR wspiera zatwierdzoną obsługę, a SOC w zadaniu 4 monitoruje i analizuje zdarzenia. Ustalenia SOC, incydenty oraz rekomendacje wracają do SZBI i SZCD STI jako dane do przeglądów, raportowania zarządczego i działań korygujących.

Zamawiający zapewni dostęp, udział właścicieli źródeł i odbiorców oraz zatwierdzenie parametrów i wyników. Wykonawca odpowiada za konfigurację i testy w zakresie przypisanym zadaniom w punktach 4.2-7.2. Poniżej określono wymagane rezultaty integracji i dowody odbioru.

I01 SZBI i SZCD STI do GRC

Właściciele, zasoby, wymagania, ryzyka i krytyczność. Dowód odbioru: powiązanie uzgodnionego rekordu ryzyka z zasobem i właścicielem; zgodność z zatwierdzonym rejestrem.

I02 Systemy IT i dopuszczone źródła OT do SIEM

Zbieranie i normalizacja logów. Dowód odbioru: odnalezienie kontrolnego zdarzenia, jego źródła, czasu i wymaganych pól w SIEM.

I03 IDS OT do SIEM

Przekazanie alertu z kontekstem urządzenia. Dowód odbioru: ten sam alert w IDS i SIEM; zachowany identyfikator źródła, czas, priorytet i opis.

I04 SIEM do SOAR do SOC

Obsługa, przypisanie, eskalacja i zatwierdzona automatyzacja. Dowód odbioru: kontrolne zdarzenie uruchamia uzgodniony scenariusz, pozostawia historię i trafia do właściwej roli.

I05 SOC i GRC do SZBI i SZCD STI

Wnioski, ryzyko, działania i raportowanie. Dowód odbioru: ustalenie ma odbiorcę, właściciela, termin i dowód wpisu do właściwego rejestru.

I06 Systemy zintegrowane do nadzoru SOC

Wykrywanie przerwy telemetrii. Dowód odbioru: kontrolowane wstrzymanie testowego źródła generuje informację o braku danych i uzgodnioną eskalację.

Rejestr integracji określa źródło, odbiorcę, właścicieli, dostęp, lokalizację danych, sposób zabezpieczenia, mapowanie pól, zależności i dowód testu. Parametry techniczne ustala się na podstawie rzeczywistej dokumentacji, bez domyślnego przypisywania nowych protokołów. Typy źródeł wskazano w niniejszym rozdziale, wymagania ich obsługi w 5.2 i 6.2, a nadzór nad brakiem telemetrii w I06 i 7.2. Dostęp SOC do danych OT musi zachować lokalne przetwarzanie wymagane w 6.2. Mapowanie pól Wykonawca dokumentuje podczas konfiguracji wymaganych integracji.

4 Zadanie 1 Szkolenia oraz obszar kompetencyjny i organizacyjny wraz z SZBI

Zadanie wzmacnia zdolność pracowników i kierownictwa do ochrony informacji oraz ciągłości dostaw wody. Rezultatem są rozwinięte kompetencje i stosowane systemy zarządzania bezpieczeństwem oraz ciągłością STI. Zasady i ryzyka wyznaczają sposób wykorzystania GRC, SIEM, SOAR, IDS OT i SOC.

4.1 Przedmiot cel i zakres

Zadanie obejmuje dziesięć pakietów usług: cztery pozycje kompetencyjne i sześć organizacyjnych, oraz usługę Security Awareness. Pakiety pozostają częściami zadania 1. Identyfikatory P4/2-P4/5 i P5/1, P5/3, P5/4, P5/5, P5/7, P5/10 oznaczają pozycje formularza, a nie dodatkowe zadania zamówienia. BCP, DRP i SZCD dotyczą STI oraz ich zależności od OT w granicach wskazanych w poszczególnych pakietach.

4.2 Zakres rzeczowy i wymagania dotyczące realizacji zadania 1

W każdym pakiecie numeracja ma charakter lokalny. Odwołania do punktów odnoszą się do danego pakietu. Produkty P1-P5 identyfikuje się łącznie z kodem pakietu. Wspólne zasady bezpieczeństwa i dokumentacji określają punkty 1.2-1.3.

Wykonawca zapewni wykonanie integracji I01 i I05 po stronie SZBI/SZCD, przy współpracy eksperta SZBI z ekspertem GRC i kierownikiem SOC, oraz przedstawi dowody określone w rozdziale 3.

Wykonawca zapewni realizację dziesięciu pakietów oraz usługi Security Awareness w zakresie określonym w 4.2, w tym produkty, testy dokumentacyjne, szkolenia, spotkania i poprawki w wymiarach określonych w pakietach.

P4/2 Szkolenia PBI i SZBI

1. Nazwa pozycji

Szkolenia dla kadry związane z wdrażaną Polityką Bezpieczeństwa Informacji i Systemem Zarządzania Bezpieczeństwem Informacji (SZBI).

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie szkolenia przekładającego Politykę Bezpieczeństwa Informacji (PBI) i zasady SZBI na codzienne obowiązki pracowników. Uczestnik ma potrafić rozpoznać sytuację wymagającą zgłoszenia, wskazać właściwy kanał kontaktu oraz zastosować zasady ochrony informacji odpowiednie do swojej roli.

3. Zakres prac

1. Wykonawca zapozna się z udostępnioną, zatwierdzoną wersją PBI, instrukcjami dla pracowników, sposobem zgłaszania incydentów i podziałem odpowiedzialności. Wskaże braki uniemożliwiające przygotowanie spójnego szkolenia.

2. Opracuje program przypisujący tematom szkolenia odpowiednie obowiązki wynikające z dokumentacji Zamawiającego. Obejmie ochronę i udostępnianie informacji, uprawnienia i konta, bezpieczne korzystanie z poczty i nośników, zasady pracy zdalnej, zgłaszanie podejrzeń naruszenia oraz współpracę z personelem IT i automatyki.

3. Przeprowadzi jedno szkolenie dla grupy określonej w pkt 10, trwające co najmniej 3 godziny. Zastosuje co najmniej trzy krótkie przypadki dotyczące obowiązków pracownika, np. omyłkowego ujawnienia dokumentu, prośby o dostęp serwisowy i podejrzanej wiadomości.

4. Przeprowadzi krótki test wiedzy przed szkoleniem i po nim, omówi odpowiedzi oraz zbierze pytania wymagające doprecyzowania procedur.

4. Sposób realizacji i współpracy

Zamawiający udostępni dokumenty wejściowe i wskaże osobę odpowiedzialną za SZBI. Program zostanie przekazany do akceptacji co najmniej 5 dni roboczych przed szkoleniem. Podstawę stanowią dokumenty z wdrożenia SZBI lub równoważne dokumenty już obowiązujące. Wykonawca nie ustanawia nowych obowiązków pracowników w materiałach szkoleniowych; propozycje zmian przekazuje właścicielowi SZBI. Forma, liczba uczestników i termin są określone w pkt 10.

5. Produkty prac

- P1 - program i materiały szkoleniowe, obejmujące skróconą instrukcję obowiązków pracownika.
- P2 - zestaw testów z kluczem odpowiedzi.
- P3 - raport realizacji z potwierdzeniem udziału, zbiorczymi wynikami testów, odpowiedziami na pytania i listą potrzebnych doprecyzowań.

6. Minimalne wymagania dotyczące produktów

P1 musi wskazywać wersję dokumentów będących podstawą szkolenia, co najmniej pięć praktycznych obowiązków i sposób zgłoszenia incydentu. P2 obejmuje co najmniej pięć pytań sprawdzających te same obszary przed szkoleniem i po nim. P3 zawiera datę, czas trwania, zrealizowane tematy i liczbę uczestników. Do materiałów i raportu stosuje się pkt 1.3. Imienną ewidencję udziału należy oddzielić od wyników zbiorczych.

7. Wymagania organizacyjne i bezpieczeństwa

Wykonawca zachowa poufność dokumentacji, ograniczy dane osobowe do ewidencji udziału i użyje przykładów testowych lub zanonimizowanych. Szkolenie odbywa się bez dostępu do produkcyjnych systemów i bez czynności zakłócających pracę operacyjną. Zamawiający może przerwać zajęcia z przyczyn bezpieczeństwa. Wyniki są przekazywane uzgodnionym, zabezpieczonym kanałem; kopie robocze zostaną zwrócone albo usunięte po odbiorze, w terminie uzgodnionym przy rozpoczęciu prac. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2.

8. Odbiór prac

Podstawą odbioru jest przeprowadzenie szkolenia w wymaganym czasie i zakresie, przekazanie P1-P3, wykonanie pomiaru wiedzy oraz zgodność instrukcji z dokumentami Zamawiającego. Wynik testu uczestnika i określony przyrost wiedzy nie stanowią warunku odbioru. Nieobecność zgłoszonych osób wymaga odnotowania, lecz nie oznacza obowiązku organizacji dodatkowego wydarzenia. Odbiór potwierdza protokół.

9. Warunki uzupełnień i poprawek

Cena obejmuje jedną skonsolidowaną rundę uwag do programu i materiałów oraz usunięcie wszystkich stwierdzonych niezgodności z OPZ. Poprawione pliki należy przekazać w ciągu 5 dni roboczych od uwag; niezgodność w przeprowadzonych zajęciach wymaga uzupełnienia brakującego zakresu w terminie uzgodnionym z Zamawiającym, bez dodatkowej opłaty.

10. Parametry realizacji

Szkolenie zapewnia udział 13 uczestników wskazanych przez Zamawiającego. Formę, miejsce lub sposób połączenia zdalnego oraz terminy grup uzgadnia się w harmonogramie w granicach terminu realizacji.

P4/3 Szkolenia specjalistyczne

1. Nazwa pozycji

Specjalistyczne szkolenia z cyberbezpieczeństwa dla kadry zarządzającej i informatyków.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest przeprowadzenie dwóch odrębnych modułów rozwijających kompetencje decyzyjne kadry zarządzającej i praktyczne kompetencje informatyków. Rezultatem ma być umiejętność oceny wpływu cyberzagrożeń na działalność wodociągową oraz doboru bezpiecznych działań organizacyjnych i technicznych w granicach odpowiedzialności uczestników.

3. Zakres prac

1. Wykonawca ustali z koordynatorem poziom wiedzy, role uczestników i istotne ryzyka na podstawie krótkiej konsultacji i przekazanych materiałów.

2. Przeprowadzi moduł dla kadry zarządzającej, trwający co najmniej 2 godziny, obejmujący: odpowiedzialność za decyzje i zasoby, ocenę i akceptację ryzyka, nadzór nad dostawcami, priorytety ciągłości dostaw wody, decyzje w incydencie oraz ocenę informacji i rekomendacji przedstawianych przez IT.

3. Przeprowadzi moduł dla informatyków, trwający co najmniej 3 godziny, obejmujący: ochronę kont uprzywilejowanych i dostępu zdalnego, analizę przykładowych alertów i logów, zabezpieczanie informacji o

incydencie, priorytetyzację podatności, planowanie bezpiecznych aktualizacji, weryfikację kopii zapasowych i współpracę z automatykami oraz dostawcami.

4. W każdym module zrealizuje jedno zadanie sytuacyjne i krótki pomiar wiedzy. Dla kierownictwa zadanie dotyczy wyboru działania i uzasadnienia ryzyka; dla IT - analizy danych testowych oraz zaplanowania reakcji z warunkami przerwania i wycofania zmian.

4. Sposób realizacji i współpracy

Program musi rozdzielać treści dla obu grup. Kontekst OT obejmuje zależności między usługami IT a automatyką, ograniczenia aktualizacji i konieczność uzgodnienia działań z eksploatacją. Nie wymaga się szkolenia z obsługi konkretnego produktu. Przy omawianiu obowiązków prawnych Wykonawca zweryfikuje ich aktualność i zastosowanie do statusu przekazanego przez Zamawiającego. Programy przekazuje do akceptacji co najmniej 5 dni roboczych przed zajęciami. Wykorzystuje się środowisko demonstracyjne Wykonawcy lub analizę przygotowanych materiałów.

5. Produkty prac

- P1 - dwa programy z materiałami dostosowanymi do obu grup.
- P2 - dwa zadania sytuacyjne z przykładowym rozwiązaniem oraz pytania sprawdzające z kluczem.
- P3 - raport realizacji z ewidencją udziału, wynikami zbiorczymi i rekomendacjami dalszego rozwoju kompetencji.

6. Minimalne wymagania dotyczące produktów

P1 wskazuje cele, tematykę i czas każdego modułu. P2 obejmuje co najmniej pięć pytań dla każdej grupy oraz kryteria oceny zadania sytuacyjnego. P3 rozdziela wyniki obu modułów, dokumentuje ich czas i zakres oraz zawiera co najmniej po jednej praktycznej rekomendacji dla każdej grupy. Do plików stosuje się pkt 1.3.

7. Wymagania organizacyjne i bezpieczeństwa

Przykłady muszą wykorzystywać dane testowe lub zanonimizowane. Zakres, terminy i zasady demonstracji podlegają wcześniejszemu uzgodnieniu. Nie dopuszcza się skanowania ani zmiany konfiguracji produkcyjnych systemów IT lub OT, prób destrukcyjnych i użycia rzeczywistych danych dostępowych. Zamawiający może przerwać demonstrację. Wykonawca zachowa poufność, przekaże materiały zabezpieczonym kanałem i zwróci albo usunie dane robocze po odbiorze w uzgodnionym terminie. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2.

8. Odbiór prac

Odbiór nastąpi po przeprowadzeniu obu modułów w wymaganym wymiarze, zrealizowaniu zadań i pomiaru wiedzy oraz przekazaniu P1-P3. Weryfikuje się oddzielną tematykę, poprawność rozwiązań i obecność wymaganych zagadnień. Nie uzależnia się odbioru od osiągnięcia określonego wyniku przez uczestników. Wykonanie potwierdza protokół.

9. Warunki uzupełnień i poprawek

Wykonawca uwzględni jedną skonsolidowaną rundę uwag do programów oraz usunie wszystkie niezgodności produktów w ciągu 5 dni roboczych od ich zgłoszenia. Pominięty wymagany temat uzupełni bez dodatkowej opłaty w terminie uzgodnionym z Zamawiającym.

10. Parametry realizacji

Moduł dla kadry zarządzającej zapewnia udział 13 uczestników wskazanych przez Zamawiającego. Moduł dla informatyków zapewnia udział 2 uczestników wskazanych przez Zamawiającego. Formę, miejsce lub sposób połączenia zdalnego oraz terminy grup uzgadnia się w harmonogramie w granicach terminu realizacji.

P4/4 Szkolenie i test socjotechniczny

1. Nazwa pozycji

Szkolenia z cyberbezpieczeństwa powiązane z testami socjotechnicznymi.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest jeden autoryzowany test socjotechniczny w kanale poczty elektronicznej, analiza wyników oraz szkolenie odnoszące się do zaobserwowanych zachowań. Celem jest poprawa rozpoznawania podejrzanych wiadomości i ich zgłaszania z poszanowaniem godności i prywatności pracowników.

3. Zakres prac

1. Wykonawca opracuje plan testu obejmujący jedną kampanię i jeden scenariusz wiadomości, grupę adresatów, maksymalnie 5 dni roboczych obserwacji, zakres mierzonych zdarzeń, zasady wyłączenia osób i procedurę natychmiastowego zatrzymania.

2. Uzyska pisemną autoryzację uprawnionej osoby Zamawiającego i przeprowadzi próbę techniczną na wskazanym koncie testowym. Uzgodni z obsługą IT sposób rozpoznawania zgłoszeń dotyczących symulacji.

3. Przeprowadzi kampanię w zatwierdzonym oknie. Dopuszcza się neutralną wiadomość z odnośnikiem do bezpiecznej strony edukacyjnej, która nie zawiera formularza pozyskiwania haseł ani danych służbowych.

4. Przeanalizuje dostarczenia, unikalne interakcje i prawidłowe zgłoszenia, uwzględniając błędy doręczeń i możliwe automatyczne otwieranie odnośników przez zabezpieczenia poczty.

5. W ciągu 10 dni roboczych od zamknięcia kampanii przeprowadzi jedno szkolenie trwające co najmniej 2 godziny. Omówi sygnały ostrzegawcze, zasady weryfikacji nadawcy i sposób zgłoszenia. Sprawdzi wiedzę krótkim quizem.

4. Sposób realizacji i współpracy

Zamawiający wskaże koordynatora, uprawnionego autora zgody, kontakty do przerwania testu i osoby mogące otrzymać wyniki. Przed startem strony ustalą role w przetwarzaniu danych, niezbędne podstawy i obowiązki informacyjne; udział właściwej osoby do spraw ochrony danych zapewnia Zamawiający. Wymagana dokumentacja powierzenia, jeżeli jest potrzebna, musi zostać zawarta przed udostępnieniem danych. Dokładny scenariusz może pozostać nieznany uczestnikom do zakończenia testu, przy zachowaniu uzgodnionych obowiązków informacyjnych. P4/4 obejmuje jedną kampanię i jedno szkolenie po teście. Jeśli kampania zostanie wykonana na platformie Security Awareness, ten sam zakres realizuje się i rozlicza tylko raz. Usługa platformy trwa 6 miesięcy zgodnie z odrębnym zakresem w 4.2; nie zastępuje pozostałych szkoleń ani ćwiczenia tabletop.

5. Produkty prac

• P1 - plan i scenariusz testu wraz z zapisem autoryzacji i próby technicznej.

• P2 - zagregowany raport wyników i rekomendacji.

• P3 - materiały szkolenia po teście, quiz z kluczem i potwierdzenie realizacji zajęć.

6. Minimalne wymagania dotyczące produktów

P2 poda liczby bezwzględne, mianowniki i definicje wskaźników. Odsetek interakcji i zgłoszeń oblicza się wobec liczby unikalnych adresatów, do których wiadomość została dostarczona; ograniczenia identyfikacji automatycznych kliknięć muszą być opisane. Samo otwarcie wiadomości nie jest dowodem błędu pracownika. Raport nie zawiera imiennych rankingów; grupy umożliwiające identyfikację pojedynczych osób łączy się w większe agregaty. P3 zawiera co najmniej pięć pytań i omówienie prawidłowych reakcji. Produkty są przekazywane po polsku w wersji edytowalnej i PDF, do wykorzystania i aktualizacji przez Zamawiającego.

7. Wymagania organizacyjne i bezpieczeństwa

Zabrania się działań fizycznie niebezpiecznych, wywoływania alarmów, podszywania się pod służby publiczne, żądania rzeczywistych haseł, instalowania złośliwego oprogramowania oraz oddziaływania na produkcyjne systemy OT. Nie wolno wyłączać zabezpieczeń poczty dla całej organizacji. Ewentualny wyjątek techniczny musi być ściśle ograniczony, zatwierdzony i wycofany po teście. Nie stosuje się gróźb utraty pracy ani tematów zdrowia i tragedii osobistych.

Uprawniona osoba Zamawiającego może natychmiast przerwać test. Rzeczywiste zgłoszenie incydentu zachowuje pierwszeństwo i nie może zostać automatycznie odrzucone jako element symulacji. Krytyczne zagrożenie zgłasza się niezwłocznie ustalonym kanałem. Dane indywidualne dostępne są wyłącznie osobom wskazanym w planie, w minimalnym zakresie potrzebnym do analizy; wyniki mają cel edukacyjny, bez publicznego piętnowania i automatycznych konsekwencji pracowniczych. Przekazanie danych odbywa się

szyfrowanym kanałem. Po uzgodnionym okresie retencji należy usunąć identyfikatory, adresy, tokeny i kopie robocze oraz potwierdzić usunięcie; materiały szkoleniowe wykorzystują dane zanonimizowane.

8. Odbiór prac

Odbiór obejmuje weryfikację autoryzacji, przeprowadzenia kampanii według zatwierdzonego planu, rzetelności wskaźników, wykonania szkolenia i kompletności P1-P3. Potwierdzenie usunięcia danych dołącza się do dokumentacji w terminie retencji. Nie wymaga się minimalnego odsetka kliknięć ani poprawy wskaźników jako warunku odbioru. W przypadku przerwania testu strony dokumentują wykonany zakres i ustalają bezpieczne wznowienie pozostałej części.

9. Warunki uzupełnień i poprawek

Cena obejmuje jedną rundę uzgodnienia scenariusza oraz usunięcie wszystkich niezgodności raportu i materiałów w ciągu 5 dni roboczych. W razie błędu technicznego po stronie Wykonawcy przeprowadzi on ponownie wyłącznie niewykonaną prawidłowo część, po nowej autoryzacji i bez dodatkowej opłaty.

10. Parametry realizacji

Kampania obejmuje 60 użytkowników, z uwzględnieniem wyłączeń bezpieczeństwa zatwierdzonych w planie testu. Szkolenie po teście zapewnia udział 60 uczestników wskazanych przez Zamawiającego. Formę, miejsce lub sposób połączenia zdalnego i okno kampanii uzgadnia się w harmonogramie, z zachowaniem terminów określonych w pkt 3.

P4/5 Ćwiczenie symulacyjne

1. Nazwa pozycji

Szkolenia symulacyjne z zakresu cyberbezpieczeństwa, ciągłości działania i zarządzania kryzysowego.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie jednego moderowanego ćwiczenia warsztatowego typu tabletop, czyli omówienia decyzji i działań na podstawie rozwijanego scenariusza. Celem jest sprawdzenie współpracy kierownictwa, personelu IT, automatyki i osób odpowiedzialnych za komunikację podczas zakłócenia, które może wpływać na dostawy wody.

3. Zakres prac

1. Wykonawca zapozna się z przekazanymi zasadami reagowania, planami ciągłości działania (BCP), planami odtwarzania po awarii (DRP) i podziałem ról. Brakujące elementy oznaczy jako założenia ćwiczenia.

2. Przygotuje jeden scenariusz cyberincydentu wpływającego na dostępność wskazanej usługi teleinformatycznej i możliwość współpracy z eksploatacją. Scenariusz obejmie co najmniej cztery kolejne informacje sytuacyjne: wykrycie, eskalację, ograniczenie dostępności i decyzję o odtworzeniu.

3. Przeprowadzi ćwiczenie trwające co najmniej 3 godziny, łącznie z omówieniem. Uczestnicy przećwiczą rozpoznanie zdarzenia, podział odpowiedzialności, priorytety, współpracę z dostawcą i komunikację wewnętrzną oraz przygotowanie przykładowego komunikatu zewnętrznego.

4. Zarejestruje decyzje, opóźnienia, luki informacyjne i sporne kompetencje, a następnie omówi je z uczestnikami.

5. Opracuje listę działań usprawniających, z priorytetami, proponowanymi właścicielami, terminami i sposobem potwierdzenia wykonania.

4. Sposób realizacji i współpracy

Zamawiający wskaże uczestników reprezentujących właściwe funkcje i zapewni ich udział. Scenariusz, cele, terminy i ograniczenia zatwierdzi co najmniej 5 dni roboczych przed ćwiczeniem. Wykonawca moderuje przebieg; decyzje symulacyjne podejmują uczestnicy. Zatwierdzone BCP/DRP i zasady Systemu Zarządzania Ciągłością Działania STI stanowią dane wejściowe. Przy ich braku ćwiczenie sprawdza role i założenia, a raport nie może stwierdzać skuteczności nieistniejących planów. Ta pozycja finansuje przygotowanie, prowadzenie i raport; utrzymanie systemów zarządzania wykorzystuje jego wyniki bez ponownego rozliczenia ćwiczenia.

5. Produkty prac

• P1 - plan ćwiczenia, scenariusz, informacje sytuacyjne i kryteria obserwacji.

- P2 - materiały uczestników i zapis przebiegu oraz decyzji.
- P3 - raport z omówienia i rejestr działań usprawniających.

6. Minimalne wymagania dotyczące produktów

Scenariusz musi łączyć aspekty techniczne, organizacyjne, komunikacyjne i decyzyjne. P2 identyfikuje role, przekazane informacje i reakcje na każdą z nich. P3 rozdziela obserwacje od założeń, wskazuje odwołania do testowanych procedur oraz sposób zamknięcia każdej stwierdzonej luki. Jeżeli nie zidentyfikowano luki w danym obszarze, raport podaje podstawę oceny. Do dokumentów stosuje się pkt 1.3.

7. Wymagania organizacyjne i bezpieczeństwa

Ćwiczenie nie może wywoływać rzeczywistego incydentu, alarmu ani przerwy w pracy systemów. Zabrania się zmian nastaw, sterowania urządzeniami, wysyłania komunikatów do rzeczywistych odbiorców zewnętrznych i wykonywania prób destrukcyjnych. Materiały należy oznaczyć „ĆWICZENIE”. Stosuje się dane testowe lub zanonimizowane; kontakty do służb i dostawców odgrywa moderator. Rzeczywiste zagrożenie ma pierwszeństwo, a Zamawiający może przerwać ćwiczenie. Wykonawca zgłasza krytyczne ustalenia wyznaczonej osobie, chroni dokumentację, przekazuje wyniki bezpiecznym kanałem i usuwa albo zwraca dane robocze po odbiorze w uzgodnionym terminie.

8. Odbiór prac

Odbiór obejmuje przeprowadzenie wymaganego czasu zajęć, podanie czterech informacji sytuacyjnych, udokumentowanie decyzji, omówienie ćwiczenia i przekazanie P1-P3. Kryterium stanowi jakość udokumentowania przebiegu i wniosków, nie bezbłędne działanie uczestników. Raport nie potwierdza technicznego osiągnięcia czasów odtworzenia na podstawie samej dyskusji. Odbiór dokumentuje protokół.

9. Warunki uzupełnień i poprawek

Wykonawca uwzględni jedną skonsolidowaną rundę uwag do scenariusza. Raport przekaże do 5 dni roboczych po ćwiczeniu, a wszystkie niezgodności produktów usunie w ciągu 5 dni roboczych od ich zgłoszenia. Brak wymaganej części ćwiczenia wynikający z działania Wykonawcy wymaga jej uzupełnienia w uzgodnionym terminie bez dodatkowej opłaty.

10. Parametry realizacji

Szkolenie symulacyjne w formie ćwiczenia tabletop zapewnia udział 15 uczestników wskazanych przez Zamawiającego. Obsadę ról określa pkt 4. Formę, miejsce lub sposób połączenia zdalnego oraz terminy grup uzgadnia się w harmonogramie w granicach terminu realizacji.

Usługa Security Awareness - platforma szkoleniowa i kampanie edukacyjne

Wykonawca zapewni w zadaniu 1 usługę Security Awareness dla 60 użytkowników Zamawiającego przez 6 miesięcy od uruchomienia usługi i udostępnienia kont. Zakres obejmuje platformę szkoleniową, platformę phishingową, raportowanie oraz przygotowanie i realizację kampanii edukacyjnej zgodnie z poniższymi wymaganiami. Kampanię socjotechniczną z P4/4 realizuje się i rozlicza jednokrotnie, także gdy wykorzystuje tę platformę.

Platforma szkoleniowa udostępnia minimum 60 szkoleń w języku polskim, w postaci filmów i prezentacji zakończonych testami lub quizami. Łączny czas wszystkich materiałów wynosi co najmniej 8 godzin. Jest to wielkość katalogu, a nie wymagany czas nauki każdego użytkownika.

Tematyka obejmuje podstawy bezpiecznego Internetu, bezpieczeństwo poczty i załączników, phishing, spyware/malware, ochronę danych osobowych, hasła i menedżery haseł, bezpieczeństwo urządzeń mobilnych, MFA, pracę zdalną i biurową, media społecznościowe, socjotechnikę i zakupy w Internecie. Użytkownicy są podzieleni na grupy z indywidualnymi harmonogramami i dedykowanymi kampaniami phishingowymi.

Platforma phishingowa umożliwia generowanie i wysyłanie spreparowanych wiadomości do wszystkich użytkowników usługi: z odnośnikiem do strony, z odnośnikiem do symulowanego portalu logowania pozwalającego bezpiecznie sprawdzić gotowość użytkownika do podania loginu i hasła, z załącznikiem szyfrowanym lub nieszyfrowanym zawierającym bezpieczną symulację niebezpiecznego kodu oraz z dokumentem Word lub Excel zawierającym taką symulację. Funkcjonalność platformy nie określa liczby ani scenariuszy zamówionych kampanii. W P4/4 obowiązuje bezpieczny scenariusz określony w tym pakiecie; nie dopuszcza się pozyskiwania rzeczywistych haseł ani uruchamiania złośliwego kodu.

Platforma umożliwia automatyczne skierowanie użytkownika na dodatkowe szkolenie albo ponowne wykonanie wcześniej ukończonego szkolenia po interakcji z symulacją. Raporty obejmują status i termin wykonania szkoleń, grupy oraz wyniki quizów i testów. Raport kampanii obejmuje liczbę wysłanych wiadomości, informację, który użytkownik otworzył wiadomość, wykonał interakcję z symulacją lub otworzył załącznik, wraz ze szczegółowymi datami i czasami tych operacji oraz informacją o użytej platformie. Do interpretacji wyników i ochrony ewidencji stosuje się ograniczenia pomiaru i zasady P4/4.

Wykonawca przygotuje platformę, założy konta, sprawdzi techniczne warunki dostarczania wiadomości, zaproponuje do akceptacji harmonogram dopasowany do okresu usługi i dostarczy kampanię szkoleniową przez powiadomienia e-mail. Przekaże pełne raporty po zakończeniu każdego modułu oraz zbiorcze raporty końcowe.

Usługa obejmuje dwie zmiany harmonogramu, zakresu lub kolejności szkoleń miesięcznie oraz zmiany użytkowników w granicach 10% bazowej liczby 60, tj. dotyczące łącznie nie więcej niż 6 użytkowników w okresie usługi. Zmiana obsady kont nie zmniejsza liczby 60 dostępnych miejsc.

Usługa jest świadczona z centrum danych na terenie Unii Europejskiej. Dostawca zapewni całkowite usunięcie danych użytkowników po zakończeniu usługi. Zgłoszenia i komunikacja odbywają się po polsku w trybie 8×5 przez portal serwisowy i infolinię. Czas reakcji nie przekracza 1 godziny w godzinach wsparcia; reakcją jest połączenie telefoniczne lub odpowiedź w portalu. Wsparcie jest dostępne przez 8 godzin dziennie w dni robocze; Wykonawca przekaże godziny obsługi i dane kontaktowe przy uruchomieniu usługi.

Szkolenia są dostępne także w językach: angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim. Platforma szkoleniowa, platforma phishingowa i moduł raportowania pochodzą od jednego producenta. Podmiot świadczący usługę posiada certyfikat ISO 9001.

P5/1 Wdrożenie SZBI

1. Nazwa pozycji

Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest opracowanie lub dostosowanie do stanu organizacji i uruchomienie SZBI w zakresie określonym w pkt 10. Rezultatem ma być zestaw stosowanych zasad, odpowiedzialności i rejestrów pozwalających zarządzać ryzykiem bezpieczeństwa informacji oraz dokumentować decyzje. Wdrożenie obejmuje uzgodnione działania organizacyjne i sprawdzenie ich zastosowania.

3. Zakres prac

1. Analiza stanu istniejącego: Wykonawca przeanalizuje udostępnione dokumenty i informacje, przeprowadzi konsultacje z właścicielami procesów, IT i automatyką oraz opisze zakres SZBI, istotne informacje, usługi, zasoby i zależności. Wykorzysta dostępne inwentarze, nie wykonując aktywnego rozpoznania sieci.

2. Ocena luk: porówna stan organizacji z wymaganym zakresem SZBI, wskaże dowody, braki, skutki i priorytety. Zweryfikuje przepisy właściwe dla potwierdzonego statusu Zamawiającego i odróżni obowiązek prawny od zalecenia. Punktem odniesienia metodycznego jest ISO/IEC 27001:2022 ze zmianą Amd 1:2024 lub równoważne podejście obejmujące wymagane rezultaty; zamówienie nie obejmuje certyfikacji.

3. Zarządzanie ryzykiem: uzgodni prostą metodę oceny i akceptacji ryzyka, przeprowadzi ocenę dla zakresu objętego usługą oraz opracuje plan postępowania z ryzykiem. Dobór zabezpieczeń i odstępstwa muszą posiadać uzasadnienie oraz wskazanego właściciela decyzji.

4. Dokumentacja: przygotuje lub zaktualizuje PBI i niezbędne zasady wykonawcze: role, klasyfikację i obieg informacji, zarządzanie dostępem, incydentami, zmianami i podatnościami, współpracę z dostawcami, dostęp zdalny, kopie zapasowe i powiązanie z ciągłością działania. Wykorzysta dokumenty istniejące; nie wymaga się osobnej procedury dla każdego tematu.

5. Wdrożenie: wesprze zatwierdzenie i udostępnienie dokumentów, przypisanie właścicieli, uruchomienie rejestrów i zastosowanie nowych zasad do co najmniej dwóch przypadków, np. oceny ryzyka oraz zgłoszenia zdarzenia lub przeglądu uprawnień. Przypadki mogą być testowe, jeżeli nie wystąpiły odpowiednie zdarzenia rzeczywiste.

Punktem wejścia do prac SZBI jest istniejąca dokumentacja bezpieczeństwa oraz ustalenia audytu „0". Należy wykorzystać przydatne postanowienia istniejącej dokumentacji w ramach zakresu tego pakietu.

6. Przegląd i aktualizacja: wykona jeden przegląd po uruchomieniu, poprawi wykryte niezgodności dokumentacji i przygotuje plan dalszych działań. Przeprowadzi jedno spotkanie przekazania wiedzy dla właściciela SZBI, trwające co najmniej 2 godziny.

4. Sposób realizacji i współpracy

Wykonawca na początku przedstawi harmonogram analizy, uzgodnień, uruchomienia i odbioru. W zakresie ceny mieszczą się trzy spotkania robocze po maksymalnie 2 godziny oraz spotkanie przekazania wiedzy; pozostałe uzgodnienia odbywają się na dokumentach. Zamawiający zapewnia udział właścicieli procesów, podejmuje decyzje o akceptacji ryzyka, zatwierdza dokumenty i odpowiada za działania swoich pracowników. Wykonawca przygotowuje materiały i wspiera wykonanie uzgodnionych działań.

BCP/DRP i system zarządzania ciągłością działania są produktami odrębnych pozycji; w SZBI opisuje się ich właścicieli i powiązania. Szkolenie ogółu pracowników realizuje P4/2. Po odbiorze wersja bazowa SZBI trafia do utrzymania w P5/3. Zakupy, zmiany techniczne wymagające osobnych wdrożeń i odrębne audyty są wskazywane jako dalsze działania, a nie przedstawiane jako wykonane w tej usłudze.

5. Produkty prac

• P1 - raport stanu istniejącego, zakres SZBI i ocena luk.

• P2 - pakiet PBI i zasad wykonawczych wraz z wykazem wersji, właścicieli i zatwierdzeń.

• P3 - metoda oceny, rejestr ryzyka i plan postępowania z ryzykiem, z uzasadnieniem doboru zabezpieczeń.

• P4 - rejestr wdrożenia, wynik pierwszego przeglądu, plan dalszych działań i potwierdzenie przekazania wiedzy.

6. Minimalne wymagania dotyczące produktów

P1 musi odróżniać stan potwierdzony od informacji brakujących. P2 opisuje, kto, w jakiej sytuacji i w jakim terminie wykonuje czynność oraz gdzie pozostawia jej zapis. P3 identyfikuje ryzyko, przyczynę, możliwy skutek, istniejące zabezpieczenia, ocenę, właściciela, działanie i status akceptacji. P4 zawiera dowody dwóch zastosowań zasad, decyzje o uruchomieniu i wyniki przeglądu. Niewdrożone zabezpieczenia techniczne należy oznaczyć wraz z ryzykiem i odpowiedzialną osobą. Do produktów stosuje się pkt 1.3; aktualizacja i przekazanie następnemu wykonawcy nie mogą wymagać zakupu dodatkowego narzędzia.

7. Wymagania organizacyjne i bezpieczeństwa

Wykonawca uzgodni zakres, terminy i zasady pozyskiwania danych. Działa na dokumentacji i informacjach przekazywanych przez uprawnione osoby; dostęp do środowiska produkcyjnego nie jest wymagany. Nie wolno wykonywać nieuzgodnionych zmian, testów destrukcyjnych ani czynności zakłócających procesy technologiczne. Zamawiający może przerwać działanie. Materiały zawierające informacje o ryzykach i zabezpieczeniach podlegają ograniczeniu dostępu oraz bezpiecznemu przekazaniu. Dane testowe lub zanonimizowane mają pierwszeństwo. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2. Kopie robocze należy zwrócić albo usunąć po odbiorze w uzgodnionym terminie.

8. Odbiór prac

Odbiór wymaga kompletności P1-P4, objęcia ustalonego zakresu, uzgodnionych właścicieli i decyzji, udokumentowania dwóch zastosowań zasad, przeprowadzenia przeglądu oraz przekazania wiedzy. Dokumenty muszą być wzajemnie spójne, a istotne luki jawnie przedstawione do decyzji. Odbiór wdrożenia następuje po zatwierdzeniu dokumentów przez uprawnioną osobę Zamawiającego; samo dostarczenie wzorców nie oznacza wdrożenia. Otwarte, zaakceptowane działania techniczne pozostają w planie i nie mogą być opisane jako zakończone. Odbiór potwierdza protokół z wykazem przyjętych wersji.

9. Warunki uzupełnień i poprawek

Cena obejmuje dwie skonsolidowane rundy uwag do dokumentacji oraz usunięcie wszystkich niezgodności z OPZ, także wykrytych podczas pierwszego przeglądu. Termin poprawy wynosi do 10 dni roboczych od przekazania uwag, chyba że strony uzgodnią inny termin uzasadniony zakresem niezgodności. Zwiększenie zakresu organizacji nie jest poprawką dokumentacji.

10. Parametry realizacji

SZBI obejmuje środowisko Zamawiającego opisane funkcjonalnie w rozdziale 3: cztery lokalizacje, systemy SCADA, ERP, GIS i usługi pomocnicze. Klasyfikacja informacji i identyfikacja zasobów stanowią prace pakietu

P5/1. Zamawiający wskaże właścicieli procesów oraz osoby IT i automatyki uczestniczące w pracach; spotkania odbywają się w wymiarze określonym w pkt 4.

P5/3 Utrzymanie SZBI

1. Nazwa pozycji

Utrzymanie i zarządzanie SZBI.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest okresowe wsparcie Zamawiającego w utrzymaniu działającego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Rezultatem ma być aktualna dokumentacja, prowadzony rejestr ryzyka i działań oraz udokumentowany cykl przeglądów, umożliwiający kierownictwu podejmowanie decyzji o bezpieczeństwie informacji.

3. Zakres prac

1. Wykonawca przejmie zatwierdzony zakres, dokumenty i otwarte działania SZBI, potwierdzi ich wersje oraz uzgodni kalendarz utrzymania.

2. Raz w każdym miesiącu świadczenia usługi przeprowadzi przegląd przekazanych informacji o ryzykach, incydentach, zmianach, uprawnieniach, podatnościach i dostawcach. Uwzględni wpływ na usługi wodociągowe oraz zależności IT/OT. Przy braku nowych zdarzeń odnotuje ten fakt i źródło potwierdzenia.

3. Zaktualizuje rejestr ryzyka i plan działań, przygotuje potrzebne zmiany dokumentacji oraz wskaże decyzje wymagane od właścicieli. Na podstawie zamkniętych incydentów i wyników przeglądów zaproponuje działania korygujące i sprawdzi dowody ich wykonania.

4. Udzieli konsultacji dotyczących stosowania procedur i oceny wpływu zmian, w ramach ustalonego limitu godzin. Monitoruje zmiany wymagań prawnych właściwych dla potwierdzonego statusu organizacji i przedstawia wpływ na dokumenty objęte usługą.

5. Raz w okresie umowy przygotuje i wesprze przegląd zarządzania, obejmujący skuteczność działań, ryzyka, incydenty, wyniki dostępnych kontroli lub audytów, potrzeby zasobowe i cele na następny okres.

6. Na zakończenie przekaże aktualną wersję dokumentacji, historię zmian i wykaz otwartych spraw z właścicielami oraz terminami.

4. Sposób realizacji i współpracy

Utrzymanie obejmuje dokumentację SZBI odebraną w P5/1; jej wersje ujmuje się w wykazie przejętych dokumentów P1.

Warunkiem rozpoczęcia jest odebrany SZBI z P5/1. Wykonawca świadczy konsultacje w dni robocze, w godzinach 8:00-16:00; przyjęcie zgłoszenia potwierdza najpóźniej następnego dnia roboczego i ustala termin odpowiedzi stosownie do pilności. Nie jest to gwarancja usunięcia incydentu.

Miesięczny przegląd obejmuje analizę materiałów i jedno spotkanie zdalne do 1 godziny. Łączny limit godzin obejmuje przygotowanie, spotkania, aktualizacje, konsultacje, raporty i przegląd zarządzania. Stałe produkty i cykle muszą zmieścić się w tym limicie. Przy wykorzystaniu 80% puli Wykonawca informuje koordynatora; priorytety pozostałych konsultacji ustala Zamawiający. Bez odrębnego zlecenia nie powstaje obowiązek płatnych prac ponad limit.

Zamawiający przekazuje informacje, zatwierdza zmiany i ryzyko oraz wykonuje działania operacyjne. Wykonawca wspiera i dokumentuje cykl, nie przejmując decyzji kierownictwa. Techniczne reagowanie, obsługa SOC, odrębne audyty i ponowne wdrożenie SZBI nie są objęte usługą. Opracowanie wzorcowych klauzul umownych należy do P5/10, a utrzymanie BCP/DRP do P5/7.

5. Produkty prac

- P1 - plan utrzymania i wykaz przejętych dokumentów.
- P2 - miesięczne raporty utrzymania z ewidencją czynności i czasu oraz aktualizowane dokumenty i rejestry objęte zakresem.
- P3 - materiał i zapis przeglądu zarządzania wraz z decyzjami Zamawiającego.
- P4 - końcowy pakiet przekazania z wykazem otwartych spraw.

6. Minimalne wymagania dotyczące produktów

P2 zawiera okres, źródła danych, przegląd ryzyk, incydentów i zmian, działania korygujące, właścicieli, terminy oraz rozliczenie wykorzystania puli godzin. Każda zmiana dokumentu posiada wersję i uzasadnienie; brak zmiany również może być wynikiem przeglądu. P3 rozdziela rekomendacje Wykonawcy i decyzje kierownictwa. P4 zapewnia możliwość dalszego utrzymania bez zależności od Wykonawcy. Do dokumentów i rejestrów stosuje się pkt 1.3.

7. Wymagania organizacyjne i bezpieczeństwa

Zakres analizy, terminy i kanały współpracy podlegają wcześniejszemu uzgodnieniu. Prace nie wymagają aktywnego dostępu do produkcyjnych systemów ani zmian w IT/OT. Zakazane są nieuzgodnione ingerencje i próby destrukcyjne; Zamawiający może zatrzymać działanie. Wykonawca chroni informacje o zabezpieczeniach, podatnościach i osobach, stosuje dane zanonimizowane, kiedy wystarczają do analizy, i przekazuje wyniki zabezpieczonym kanałem. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2. Dane robocze zwraca albo usuwa po zakończeniu umowy w uzgodnionym terminie. Obowiązki poufności dotyczą również podwykonawców.

8. Odbiór prac

Raport miesięczny przekazuje się do 5. dnia roboczego kolejnego miesiąca; raport za ostatni okres wraz z pakietem końcowym - do 5 dni roboczych od zakończenia usługi. Odbiór okresowy sprawdza wykonanie zaplanowanego cyklu, aktualność rejestrów, kompletność raportu i rozliczenie czasu. Końcowy odbiór obejmuje P1-P4 i przeprowadzenie przeglądu zarządzania. Niezakończone działania Zamawiającego są wykazywane jako otwarte i nie mogą być raportowane jako skutecznie wykonane.

9. Warunki uzupełnień i poprawek

Wykonawca usuwa niezgodności raportów i aktualizacji w ciągu 5 dni roboczych od zgłoszenia. Poprawki wynikające z nienależytego wykonania nie zużywają puli konsultacyjnej. Nowe potrzeby wykraczające poza katalog dokumentów lub zakres organizacji wymagają odrębnego uzgodnienia zakresu, bez automatycznego zwiększenia wynagrodzenia.

P5/4 BCP i DRP STI

1. Nazwa pozycji

Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI).

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest opracowanie użytecznych BCP i DRP dla systemów SCADA, w tym archiwizacji i udostępniania danych procesowych, ERP i obiegu dokumentów, GIS, systemów pomocniczych, obsługi IT i dostępu zdalnego oraz usług sieciowych i kopii zapasowych opisanych w rozdziale 3. BCP określa sposób utrzymania uzgodnionego minimum działania podczas zakłócenia, a DRP - techniczną kolejność bezpiecznego odtworzenia systemów. Plany mają umożliwić podjęcie decyzji i działanie także przy niedostępności podstawowych narzędzi informatycznych.

3. Zakres prac

1. Wykonawca przeanalizuje przekazane opisy usług, zasobów, kopii zapasowych, zależności i umów wsparcia. Ustali z właścicielami procesów skutki niedostępności oraz minimalny poziom działania niezbędny dla usług wodociągowych.

2. Przeprowadzi uproszczoną analizę wpływu zakłócenia na działalność (BIA), obejmującą skutki narastające w czasie, okresy szczególnej wrażliwości, zależności IT/OT, personel, łączność, zasilanie i dostawców. Zakres OT ogranicza się do zależności istotnych dla wskazanych STI i bezpiecznego wznowienia procesów.

3. Zaproponuje priorytety i parametry: RTO - docelowy czas przywrócenia wymaganej funkcji; RPO - dopuszczalny okres utraty danych; maksymalny tolerowany czas zakłócenia i minimalny poziom usługi. Wyraźnie określi początek pomiaru, jednostki i warunki osiągnięcia. Wartości wymagają zatwierdzenia przez właścicieli usług i nie mogą być wywodzone wyłącznie z częstotliwości kopii zapasowych.

Analiza BCP/DRP uwzględnia istniejące kopie zapasowe serwerów, stacji roboczych i usług zewnętrznych, pamięć NAS, nośniki taśmowe, replikację maszyn wirtualnych oraz wyniki sprawdzeń odtworzeń, a także zależności

systemów objętych zakresem pakietu. Częstotliwość kopii i replikacji nie jest samodzielnym potwierdzeniem osiągnięcia RTO/RPO.

4. Opracuje BCP obejmujące przesłanki uruchomienia, role i zastępstwa, działania zastępcze, komunikację, zasoby, zależności od dostawców i warunki powrotu do normalnej pracy.

5. Opracuje DRP obejmujące warunki rozpoczęcia, ocenę bezpieczeństwa środowiska, wybór i sprawdzenie kopii, kolejność odtworzenia zależnych komponentów, walidację integralności i funkcji, warunki przerwania, wycofania i przekazania systemu do eksploatacji.

6. Przeprowadzi jedną wspólną weryfikację dokumentacyjną: przejście krok po kroku przez scenariusz utraty wskazanej usługi oraz sprawdzenie kompletności każdego planu z właścicielem. Usunie niespójności i przekaże wiedzę osobom odpowiedzialnym za użycie planów.

4. Sposób realizacji i współpracy

Cena obejmuje analizę dokumentacji, jedno spotkanie BIA do 2 godzin i jedno spotkanie weryfikacji oraz przekazania do 2 godzin. Pozostałe konsultacje odbywają się na dokumentach. Zamawiający zapewnia właścicieli usług, informatyków i udział automatyka przy zależnościach OT; zatwierdza priorytety, parametry i dopuszczalne działania zastępcze. Administratorzy potwierdzają poprawność instrukcji technicznych na podstawie posiadanej dokumentacji.

Wykonawca nie zakłada dostępności zapasowych zasobów ani skuteczności kopii bez potwierdzenia. Rozbieżność między oczekiwanym RTO/RPO a możliwościami ujmuje jako lukę z rekomendacją działania. BIA i plany stanowią wejście do P5/5, ćwiczenia P4/5 oraz utrzymania P5/7. Ta pozycja nie obejmuje budowy całego systemu zarządzania ciągłością, zakupów infrastruktury ani rzeczywistego odtwarzania produkcji.

5. Produkty prac

• P1 - BIA, mapa zależności, priorytety i karta zatwierdzanych parametrów odtwarzania.

• P2 - komplet BCP dla zakresu wskazanego w pkt 2 niniejszego pakietu.

• P3 - komplet DRP dla zakresu wskazanego w pkt 2 niniejszego pakietu.

• P4 - zapis weryfikacji planów i przekazania wiedzy, z rejestrem luk oraz zaleceń.

6. Minimalne wymagania dotyczące produktów

Każdy BCP i DRP musi posiadać identyfikator, wersję, właściciela, zakres, warunki aktywacji, kolejność kroków, wykonawców, potrzebne zasoby, kryteria zakończenia i sposób potwierdzenia wykonania. Można łączyć plany powiązanych systemów, jeśli każda usługa ma jednoznaczne pokrycie w spisie. DRP nie może poprzestawać na poleceniu „odtworzyć z kopii”; wskazuje lokalizację kontrolowanej instrukcji lub opisuje operacyjne kroki właściwe dla danego systemu. Hasła i klucze nie są wpisywane do planu - wskazuje się sposób uzyskania autoryzowanego dostępu.

Parametry muszą mieć status „proponowany”, „zatwierdzony” lub „niepotwierdzony technicznie” oraz wskazaną podstawę oceny. Instrukcje niedające się opracować bez brakującej dokumentacji oznacza się jako lukę, bez zastępowania ich fikcyjnymi poleceniami. Do planów stosuje się pkt 1.3; wymagają również postaci umożliwiającej kontrolowane użycie offline.

7. Wymagania organizacyjne i bezpieczeństwa

Prace odbywają się na dokumentacji w uzgodnionym zakresie i terminach, bez zatrzymania systemów, uruchamiania odtwarzania i wykonywania prób destrukcyjnych. Nie wolno zmieniać konfiguracji ani nastaw automatyki. Bezpieczeństwo ludzi, procesu i jakości dostaw wody stanowi warunek wznowienia działania opisany w planach i potwierdzany przez uprawnioną eksploatację. Zamawiający może przerwać czynność weryfikacyjną. Stosuje się dane testowe lub zanonimizowane, ograniczony dostęp do informacji i bezpieczne przekazanie produktów. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2. Dane robocze są zwracane albo usuwane po odbiorze w uzgodnionym terminie.

8. Odbiór prac

Warunkiem odbioru jest pokrycie całego uzgodnionego katalogu usług i systemów, kompletność P1-P4, zatwierdzenie priorytetów i parametrów przez Zamawiającego oraz przeprowadzenie weryfikacji dokumentacyjnej. Każdy plan musi określać wykonalne działania i zależności. Istotny brak instrukcji uniemożliwiający wykonanie planu wymaga uzupełnienia przed odbiorem. Techniczna nieosiągalność

oczekiwanego parametru wymaga jawnej decyzji właściciela o zmianie celu albo planie usunięcia luki; nie może być przedstawiona jako spełnienie parametru. Przejście dokumentacyjne nie jest dowodem osiągnięcia RTO/RPO w środowisku produkcyjnym.

9. Warunki uzupełnień i poprawek

Cena obejmuje dwie skonsolidowane rundy uwag i usunięcie wszystkich niezgodności z OPZ w terminie do 10 dni roboczych od zgłoszenia. Dodanie kolejnych systemów lub usług ponad katalog wskazany w zamówieniu wymaga odrębnego ustalenia zakresu.

P5/5 Wdrożenie SZCD STI

1. Nazwa pozycji

Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD STI).

Zakres STI objętych SZCD odpowiada katalogowi usług i systemów wskazanemu w pkt 2 pakietu P5/4; wykorzystuje się BIA oraz BCP/DRP opracowane w tym pakiecie.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest ustanowienie i uruchomienie zasad zarządzania ciągłością działania systemów teleinformatycznych (STI) objętych katalogiem usług i systemów wskazanym w pkt 2 pakietu P5/4. Rezultatem ma być możliwy do utrzymania SZCD STI, który określa odpowiedzialności, nadzór nad planami, ćwiczenia, przeglądy i aktualizacje. Punktem odniesienia metodycznego jest ISO 22301:2019 ze zmianą Amd 1:2024 lub równoważne podejście obejmujące wymagane rezultaty; usługa nie obejmuje certyfikacji.

3. Zakres prac

1. Wykonawca przeanalizuje istniejące zasady ciągłości, zatwierdzoną analizę wpływu zakłóceń na działalność (BIA), plany ciągłości (BCP), plany odtwarzania (DRP) i powiązania z Systemem Zarządzania Bezpieczeństwem Informacji. Zidentyfikuje luki w odpowiedzialności, nadzorze i aktualizacji.

2. Ustali zakres SZCD STI, jego cele, role, zastępstwa i uprawnienia decyzyjne, w tym zasady uruchomienia i zakończenia trybu awaryjnego oraz współpracy kierownictwa, IT, automatyki i komunikacji.

3. Przygotuje zasady nadzoru nad BIA i planami: właścicieli, wersjonowanie, dystrybucję, dostępność offline, częstotliwość przeglądów i przesłanki aktualizacji po incydencie, zmianie systemu, dostawcy lub procesu.

Przy wskazywaniu ról i odpowiedzialności należy uwzględnić zastępstwa dla osób IT, automatyki i odtworzenia oraz dostępność potrzebnej dokumentacji.

4. Ustali sposób planowania i oceny ćwiczeń, prowadzenia działań korygujących, raportowania oraz przeglądu zarządzania. Przygotuje pierwszy plan działań na 12 miesięcy jako dokument planistyczny, bez obowiązku 12-miesięcznego świadczenia usługi.

5. Wesprze wdrożenie: zatwierdzenie zasad, przypisanie właścicieli, uruchomienie rejestru planów i usprawnień oraz udostępnienie aktualnych wersji osobom odpowiedzialnym.

6. Sprawdzi na jednym przykładzie zgłoszonej lub testowej zmiany, czy działa ścieżka aktualizacji planu, zatwierdzenia i przekazania nowej wersji. Przeprowadzi pierwszy przegląd działania SZCD STI, wprowadzi korekty i przekaże wiedzę właścicielowi systemu.

4. Sposób realizacji i współpracy

Wykonawca przeprowadzi dwa spotkania robocze po maksymalnie 2 godziny oraz jedno spotkanie przekazania wiedzy trwające co najmniej 1 godzinę. Zamawiający zapewnia właściciela ciągłości, właścicieli usług i udział IT oraz eksploatacji; zatwierdza zasady, cele i kompetencje decyzyjne. Wykonawca organizuje uruchomienie nadzoru i dokumentuje dowody zastosowania zasad.

Wykorzystuje się BIA i BCP/DRP z P5/4 albo równoważne, istniejące materiały. Wykonawca rejestruje je i sprawdza spójność, lecz nie opracowuje ponownie treści operacyjnej planów. Brak tych danych należy ustalić przed rozpoczęciem wdrożenia i zapewnić ich dostarczenie w ramach właściwej pozycji. Ćwiczenie kryzysowe prowadzi P4/5; sprawdzenie obiegu aktualizacji w tej pozycji jest odrębną, krótką weryfikacją mechanizmu zarządzania. Po odbiorze system przechodzi do utrzymania w P5/7.

5. Produkty prac

• P1 - zakres SZCD STI i ocena luk zarządczych.

- P2 - zasady ciągłości działania STI, odpowiedzialności i nadzoru nad dokumentacją.
- P3 - rejestr BIA i planów, rejestr usprawnień oraz plan przeglądów i ćwiczeń na 12 miesięcy.
- P4 - raport uruchomienia, wynik pierwszego przeglądu i weryfikacji obiegu zmiany oraz potwierdzenie przekazania wiedzy.

6. Minimalne wymagania dotyczące produktów

P2 wskazuje właścicieli i zastępstwa, ścieżki decyzji i komunikacji oraz powiązania z SZBI. P3 zawiera identyfikatory, wersje, daty zatwierdzeń i następnych przeglądów dokumentów, a dla usprawnień - priorytety, właścicieli, terminy i dowody zamknięcia. Plan ćwiczeń określa cel, zakres, role i sposób oceny, bez domyślnego zezwolenia na ingerencję techniczną. Minimalne miary to aktualność przeglądów planów i terminowość działań usprawniających; każda miara ma definicję i źródło danych. P4 odróżnia elementy uruchomione od działań pozostających do wykonania. Do produktów stosuje się pkt 1.3.

7. Wymagania organizacyjne i bezpieczeństwa

Zakres i terminy czynności uzgadnia się z Zamawiającym, zapewniając brak zakłóceń procesów technologicznych. Nie wykonuje się prób destrukcyjnych, zatrzymania produkcji ani nieuzgodnionego dostępu do systemów. Zamawiający może przerwać weryfikację. Przykład zmiany powinien wykorzystywać dane testowe albo zanonimizowane. Informacje o zależnościach, kontaktach i zasobach awaryjnych mają ograniczony dostęp; wyniki są przekazywane bezpiecznym kanałem. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2. Kopie robocze podlegają zwrotowi albo usunięciu po odbiorze w uzgodnionym terminie.

8. Odbiór prac

Odbiór wymaga zatwierdzenia zakresu i zasad przez Zamawiającego, przypisania właścicieli i zastępstw, objęcia rejestrem wszystkich przekazanych planów z ustalonego zakresu, przeprowadzenia weryfikacji obiegu zmiany i pierwszego przeglądu oraz przekazania P1-P4. Sam zestaw niezatwierdzonych szablonów nie stanowi wdrożenia. Weryfikuje się mechanizmy zarządzania; odbiór nie potwierdza technicznej skuteczności odtwarzania STI.

9. Warunki uzupełnień i poprawek

Cena obejmuje dwie skonsolidowane rundy uwag do zasad i rejestrów oraz usunięcie wszystkich niezgodności w ciągu 10 dni roboczych od zgłoszenia. Niespójności wykryte przy uruchomieniu lub pierwszym przeglądzie usuwa się przed odbiorem, bez odrębnego wynagrodzenia.

P5/7 Utrzymanie SZCD STI

1. Nazwa pozycji

Utrzymanie i zarządzanie SZCD STI.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest cykliczne wsparcie utrzymania Systemu Zarządzania Ciągłością Działania systemów teleinformatycznych (SZCD STI), wraz z aktualizacją dokumentów objętych wskazanym katalogiem. Celem jest zachowanie aktualności ról, zależności i planów oraz doprowadzanie wniosków z ćwiczeń i zakłóceń do decyzji i działań usprawniających.

3. Zakres prac

1. Wykonawca przejmie dokumentację odebranego SZCD STI, analizę wpływu zakłóceń (BIA), plany ciągłości działania (BCP), plany odtwarzania po awarii (DRP) i otwarte działania. Uzgodni harmonogram utrzymania.

2. Raz w każdym miesiącu dokona przeglądu zmian zgłoszonych przez właścicieli usług, IT, automatykę i dostawców, pod kątem ich wpływu na ciągłość. Sprawdzi aktualność odpowiedzialności, kontaktów i dostępności kontrolowanej kopii planów.

3. Raz na kwartał dokona udokumentowanego przeglądu katalogu BIA i planów oraz statusu usprawnień. Jeżeli umowa trwa krócej niż kwartał, przeprowadzi jeden taki przegląd w jej okresie. Zmiany krytyczne dla wykonalności planu analizuje bez oczekiwania na przegląd kwartalny, w ramach ustalonych zasad zgłoszeń i puli godzin.

4. Zaktualizuje objęte zakresem dokumenty i zależności, przedstawi potrzebę zmiany parametrów odtworzeniowych do zatwierdzenia właścicielom oraz sprawdzi dowody wykonania działań korygujących.

5. Zapewni wsparcie jednego ćwiczenia: przegląd celów i kryteriów przed ćwiczeniem, analizę przekazanego raportu i wprowadzenie wniosków do rejestru działań. Jeżeli ćwiczenie jest realizowane w P4/5, jego przygotowanie, moderowanie i raport są rozliczane wyłącznie w P4/5.

Przeglądy uwzględniają istniejące mechanizmy kopii i replikacji wskazane w opisie środowiska, wyniki odtworzeń oraz zmiany zależności od dostawców i dostępności dokumentacji.

6. Raz w okresie umowy wesprze przegląd zarządzania ciągłością, przedstawiając aktualność planów, wyniki ćwiczeń, zakłócenia, ryzyka i potrzeby zasobowe. Na końcu przekaże dokumentację i otwarte sprawy.

Utrzymanie obejmuje SZCD STI przekazany z P5/5 oraz BIA i BCP/DRP z P5/4; dokumenty ujmuje się w wykazie przejęcia.

4. Sposób realizacji i współpracy

Warunkiem rozpoczęcia jest przekazanie systemu z P5/5 oraz katalogu dokumentów określonego powyżej. Przegląd miesięczny obejmuje analizę materiałów i jedno spotkanie zdalne do 1 godziny. Obsługa zgłoszeń odbywa się w dni robocze w godzinach 8:00-16:00; przyjęcie potwierdza się najpóźniej następnego dnia roboczego, z ustaleniem terminu analizy.

Pula godzin obejmuje wszystkie przeglądy, przygotowanie, spotkania, aktualizacje, wsparcie ćwiczenia i raportowanie. Stałe produkty muszą zmieścić się w tej puli; przy jej wykorzystaniu w 80% Wykonawca informuje Zamawiającego i uzgadnia priorytety pozostałych konsultacji. Nie nalicza dodatkowych opłat bez odrębnego zlecenia. Jeżeli przegląd kwartalny, końcowy i przegląd zarządzania przypadają razem, mogą zostać przeprowadzone podczas jednego spotkania z zachowaniem ich zakresu.

Zamawiający odpowiada za decyzje, wykonanie zmian technicznych, zapewnienie zasobów awaryjnych oraz organizację ćwiczenia. Wykonawca nie przejmuje dyżuru kryzysowego ani technicznego odtwarzania. Usługa nie obejmuje ponownego wdrożenia SZCD ani tworzenia planów dla nowych systemów poza uzgodnionym katalogiem. Brak udostępnionego ćwiczenia wymaga udokumentowania przeszkody i ustalenia terminu, a nie wykazania fikcyjnego wykonania wsparcia.

5. Produkty prac

- P1 - plan utrzymania z wykazem przejętych BIA, BCP, DRP i dokumentów SZCD STI.
- P2 - miesięczne raporty z ewidencją czynności i czasu, obejmujące również wyniki przeglądów kwartalnych, oraz aktualne dokumenty i rejestr zmian.
- P3 - zapis wsparcia ćwiczenia, rejestr usprawnień i materiał z przeglądu zarządzania.
- P4 - końcowy pakiet przekazania z otwartymi sprawami i terminami kolejnych przeglądów.

6. Minimalne wymagania dotyczące produktów

P2 identyfikuje zmienione zależności, wersje planów, uzasadnienia zmian, osoby zatwierdzające i wykonanie terminów. Dla parametrów odtworzeniowych odnotowuje zatwierdzone cele oraz dowody lub ograniczenia ich technicznego potwierdzenia. P3 wiąże każdą rekomendację z ustaleniem ćwiczenia lub przeglądu i wskazuje właściciela, termin oraz kryterium zamknięcia. P4 pozwala odtworzyć aktualny stan nadzoru. Do dokumentów stosuje się pkt 1.3.

7. Wymagania organizacyjne i bezpieczeństwa

Analiza i aktualizacje odbywają się w uzgodnionych terminach, bez ingerencji w działające systemy IT/OT i bez prób destrukcyjnych. Czynności techniczne opisane w planach mogą być wykonane wyłącznie przez uprawnionych wykonawców w odrębnie autoryzowanym zakresie. Zamawiający może zatrzymać każdą czynność zagrażającą ciągłości. Wykonawca stosuje dane testowe lub zanonimizowane, gdy są wystarczające, chroni dane o zasobach awaryjnych i kontaktach oraz przekazuje wyniki zabezpieczonym kanałem. Zgłaszanie zagrożeń odbywa się zgodnie z pkt 1.2. Po zakończeniu zwraca albo usuwa kopie robocze w uzgodnionym terminie.

8. Odbiór prac

Raporty przekazuje się do 5. dnia roboczego następnego miesiąca, a ostatni raport i pakiet końcowy - do 5 dni roboczych od zakończenia umowy. Odbiór weryfikuje wykonanie cykli, objęcie przeglądem całego katalogu w odpowiednich okresach, aktualizacje lub uzasadnienie ich braku, rozliczenie czasu oraz przypisanie usprawnień. Odbiór końcowy obejmuje również wsparcie jednego ćwiczenia i przeglądu zarządzania. Nie wymaga

potwierdzenia rzeczywistego osiągnięcia parametrów odtworzenia, jeżeli nie przeprowadzono odrębnego testu technicznego.

9. Warunki uzupełnień i poprawek

Nieprawidłowości raportów, rejestrów i aktualizacji Wykonawca usuwa w ciągu 5 dni roboczych od zgłoszenia, bez pomniejszenia puli godzin o czas poprawienia własnych błędów. Rozszerzenie katalogu o nowe plany lub zasadnicza przebudowa systemu wymaga odrębnego uzgodnienia zakresu.

10. Wsparcie powdrożeniowe

Wykonawca zapewnia dodatkowe 40 godzin wsparcia po zakończeniu projektu.

P5/10 Doradztwo kontraktowe

1. Nazwa pozycji

Doradztwo w zakresie opracowania warunków umów na wdrożenie i utrzymanie infrastruktury cyberbezpieczeństwa, obejmujące w szczególności łańcuch dostaw, infrastrukturę monitorowania i zarządzania oraz usługi zdalne.

2. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest opracowanie praktycznych wymagań i wzorcowych klauzul do umów wdrożeniowych i utrzymaniowych dla infrastruktury cyberbezpieczeństwa IT/OT. Rezultatem ma być pakiet pozwalający określić obowiązki dostawcy, mierzyć poziom usługi, kontrolować dostęp i łańcuch dostaw oraz bezpiecznie zakończyć współpracę. Ostateczna redakcja prawna dokumentów wymaga akceptacji właściwej obsługi prawnej Zamawiającego.

3. Zakres prac

1. Wykonawca przeanalizuje wskazane projekty umów, opisy usług, zasady Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), wymagania ciągłości i planowane relacje z dostawcami. Przygotuje listę luk oraz rozróżni wymagania prawne właściwe dla potwierdzonego statusu Zamawiającego od proponowanych warunków kontraktowych.

2. Opracuje wzorcowe klauzule dotyczące zakresu i odbiorów wdrożenia, utrzymania, poufności, dokumentacji, odpowiedzialności stron, podwykonawstwa i dalszych dostawców, prawa do weryfikacji oraz zakończenia umowy. Określi obowiązek identyfikacji podwykonawców mających dostęp do informacji lub systemów, zasady akceptacji istotnych zmian i przenoszenia na nich odpowiednich obowiązków bezpieczeństwa.

Materiał wejściowy obejmuje umowy utrzymania systemów sterowania, monitorowania i automatyki oraz łączności, wskazane w pkt 10. Analiza uwzględnia dostęp serwisowy w granicach zakresu tych umów.

3. Opracuje zasady obsługi podatności, aktualizacji i końca wsparcia: informowanie o zagrożeniu, ocenę wpływu, terminy zaproponowane według ryzyka, testowanie, okna serwisowe, możliwość wycofania i działania kompensacyjne. Dla OT uwzględni ograniczenia zgodności i zatwierdzenie przez osoby odpowiedzialne za proces technologiczny.

4. Przygotuje wymagania dla monitorowania i zarządzania: zakres odpowiedzialności za źródła danych i alerty, wykrywanie braku telemetrii, logowanie działań administracyjnych, spójność czasu, integralność zapisów, uprawnienia do odczytu, retencję i eksport danych oraz zasady zmian reguł i automatycznych reakcji. Wskaże, które działania wymagają uprzedniej zgody Zamawiającego.

5. Opracuje zasady obsługi incydentów przez dostawcę: przesłanki zgłoszenia, moment rozpoczęcia pomiaru czasu, kanały podstawowe i zapasowe, minimalny zakres informacji, aktualizacje zgłoszenia, zabezpieczenie dowodów, współpracę i analizę przyczyn. Terminy kontraktowe mają umożliwiać Zamawiającemu realizację jego własnych obowiązków; nie należy utożsamiać ich automatycznie z terminami ustawowymi.

6. Opracuje załącznik określający poziomy usług (SLA): klasy zdarzeń, godziny świadczenia, czas reakcji, przywrócenia działania i rozwiązania, sposób pomiaru, zależności, dopuszczalne wyłączenia, eskalację i raportowanie. Zaproponuje mechanizmy odpowiedzialności i rozliczenia naruszeń do oceny prawnej.

7. Opracuje wymagania dla uprzywilejowanego i zdalnego dostępu serwisowego, zakończenia umowy i zmiany dostawcy oraz proporcjonalną procedurę oceny dostawców z ankietą.

8. Zastosuje pakiet do umów wskazanych w pkt 10, przedstawiając propozycje zmian i uzasadnienia. Przeprowadzi warsztaty dla zakupów, obsługi prawnej i IT/OT w łącznym wymiarze co najmniej 8 godzin, w maksymalnie dwóch spotkaniach, z omówieniem sposobu stosowania produktów.

4. Sposób realizacji i współpracy

Całość należy wykonać do 18 grudnia 2026 r. Wykonawca zakończy analizę i przedstawi projekty klauzul, SLA i zasad dostępu; procedurę oceny dostawców i wyniki konsultacji; ostateczne produkty i warsztaty. Zamawiający udostępni materiały na początku prac; terminy warsztatów uzgadnia się w harmonogramie z zachowaniem powyższych terminów.

Zamawiający wskazuje zamknięty zestaw umów do analizy, decydentów technicznych i obsługę prawną. Wykonawca wyjaśnia konsekwencje proponowanych wariantów, a Zamawiający ustala poziomy ryzyka, wymagane czasy, odpowiedzialność i koszty. Nie zakłada się automatycznie usługi całodobowej, zakupu systemu zarządzania dostępem ani nagrywania każdej sesji niezależnie od potrzeb. Obowiązki ujmuje się funkcjonalnie, odpowiednio do krytyczności usługi i możliwości środowiska. Usługa nie obejmuje stałego pełnienia funkcji pełnomocnika ani bieżącej oceny wszystkich przyszłych dostawców.

5. Produkty prac

- P1 - wzorcowy pakiet klauzul cyberbezpieczeństwa z instrukcją doboru do rodzaju umowy.
- P2 - wzorcowy załącznik SLA i bezpieczeństwa.
- P3 - procedura i ankieta oceny ryzyka dostawców wraz z zasadami oceny odpowiedzi.
- P4 - zasady zdalnego i uprzywilejowanego dostępu serwisowego IT/OT do wykorzystania jako załącznik umowny.
- P5 - raport z analizy wskazanych umów i propozycje zmian oraz materiały i potwierdzenie warsztatów.

6. Minimalne wymagania dotyczące produktów

P1 musi zawierać gotowe do adaptacji postanowienia, a nie sam wykaz zagadnień. Dla każdego postanowienia należy wskazać zakres stosowania, powiązanie z ryzykiem i pola do ustalenia w konkretnej umowie. Klauzule zakończenia współpracy obejmują okres i zakres pomocy przejściowej, eksport danych i konfiguracji w użytecznej postaci, przekazanie dokumentacji i uprawnień, unieważnienie dostępów oraz potwierdzony zwrot lub usunięcie danych i kopii według ustalonego harmonogramu. Prawa do opracowań i konfiguracji należy określić stosownie do przedmiotu; nie wymaga się bez uzasadnienia kodu źródłowego gotowych produktów.

P2 musi określać początek, koniec i zasady ewentualnego zawieszenia każdego pomiaru SLA, źródło dowodów, odpowiedzialną stronę i sposób rozstrzygania rozbieżności. Przykładowe wartości są wyraźnie oznaczane jako propozycje do zatwierdzenia, a nie jako obowiązujące ustalenia Zamawiającego. Należy sprawdzić spójność SLA z priorytetami odtwarzania i zależnościami od innych usług.

P3 obejmuje kwalifikację krytyczności dostawcy, zakres dostępu, istotnych podwykonawców, wymagane dowody, ocenę odpowiedzi i działania wobec stwierdzonych braków. Dowodami mogą być opisy procesów, wyniki kontroli lub certyfikaty; nie wolno uzależniać każdej oceny wyłącznie od posiadania konkretnego certyfikatu.

P4 określa autoryzację osoby i celu, minimalne uprawnienia, czas dostępu, uwierzytelnianie wieloskładnikowe tam, gdzie możliwe technicznie, rejestrowanie i rozliczalność działań, zasady urządzeń serwisowych oraz natychmiastowe odebranie dostępu. Wyjątek wynikający z ograniczeń OT wymaga oceny ryzyka, środków kompensacyjnych, zatwierdzenia i terminu ponownego przeglądu; nie stanowi zgody na niekontrolowane połączenie.

P5 zawiera dla każdej analizowanej umowy odniesienie do konkretnego punktu, proponowaną zmianę, uzasadnienie i status decyzji. Pakiet musi obejmować audytowalność i proporcjonalne prawo weryfikacji obowiązków dostawcy, ochronę danych, dostęp organów uprawnionych oraz zasady poufności dowodów. Wszystkie produkty należy przekazać w języku polskim, w plikach edytowalnych i PDF, z prawem adaptacji oraz wykorzystania w kolejnych umowach Zamawiającego.

7. Wymagania organizacyjne i bezpieczeństwa

Wykonawca wykorzystuje dokumenty przekazane w uzgodnionym zakresie i terminie. Analiza nie uprawnia do kontaktowania się z dostawcami w imieniu Zamawiającego ani do dostępu do produkcji. Zabrania się

nieuzgodnionych ingerencji, prób destrukcyjnych i działań zakłócających proces technologiczny; Zamawiający może przerwać każdą czynność zagrażającą bezpieczeństwu.

Wykonawca zachowuje poufność cen, warunków umów i informacji o zabezpieczeniach oraz ujawnia powiązania mogące wpływać na bezstronność doradztwa. Przykłady warsztatowe powinny być zanonimizowane. Wyniki przekazuje zabezpieczonym kanałem, krytyczne zagrożenia zgłasza niezwłocznie koordynatorowi, a kopie robocze zwraca albo usuwa po zakończeniu w uzgodnionym terminie.

8. Odbiór prac

Odbiór obejmuje kompletność P1-P5, pokrycie wszystkich obszarów wskazanych w pkt 3 i 6, analizę całego zestawu umów z pkt 10 oraz przeprowadzenie 8 godzin warsztatów. Sprawdza się, czy klauzule nadają się do adaptacji, wskaźniki SLA są mierzalne, obowiązki stron i podwykonawców są jednoznaczne, a propozycje nie wymagają wskazanego produktu bez uzasadnienia. Ostateczna redakcja prawna musi zostać zaakceptowana przez właściwą obsługę prawną Zamawiającego przed wykorzystaniem w umowach. Odbiór usługi nie oznacza zatwierdzenia z góry wszystkich przyszłych umów ani gwarancji zgodności całego przedsiębiorstwa.

9. Warunki uzupełnień i poprawek

Cena obejmuje dwie skonsolidowane rundy uwag, w tym uwagi obsługi prawnej i IT/OT, oraz usunięcie wszystkich niezgodności z OPZ. Wykonawca przekaże poprawione produkty w ciągu 10 dni roboczych od otrzymania uwag, z zachowaniem harmonogramu końcowego uzgodnionego dla terminowo przekazanych danych. Rozszerzenie zestawu analizowanych umów wymaga odrębnego ustalenia zakresu.

10. Parametry realizacji

Analiza obejmuje cztery umowy wskazane w audycie „0”: jedną dotyczącą utrzymania systemów sterowania, monitorowania i automatyki, jedną dotyczącą usług telekomunikacyjnych oraz dwie dotyczące dzierżawy włókien światłowodowych, wraz z ich obowiązującymi załącznikami i aneksami. Zamawiający udostępni dokumenty na początku prac i wskaże uczestników warsztatów z obszaru zakupów, obsługi prawnej i IT/OT. Wymiar i liczbę spotkań określa pkt 3, a terminy pkt 4.

11. Wsparcie powdrożeniowe

Wykonawca zapewnia dodatkowe 40 godzin wsparcia po zakończeniu projektu.

Wspólne wymagania realizacyjne zadania 1

Wykonawca przekaże do konfiguracji GRC uzgodnione dane o zasobach, wymaganiach, ryzykach, zabezpieczeniach i właścicielach. Integracja nie zastępuje akceptacji ryzyka i zatwierdzania dokumentów przez Zamawiającego. Rejestry muszą umożliwiać zachowanie wskazanych rezultatów niezależnie od narzędzia, z uwzględnieniem zasad zadania 2.

Wykonawca przekaże aktualne dokumenty, historię zmian, rejestry, dowody przeglądów oraz listę otwartych spraw z właścicielami i terminami. Wykonawca zapewni wycofanie własnych dostępów i potwierdzenie zwrotu albo usunięcia danych w uzgodnionych terminach.

4.3 Etapy integracje i przekazanie wiedzy

Kolejność etapów obejmuje: analizę stanu i luk, uzgodnienie zakresów i metod, przygotowanie dokumentacji, wdrożenie zasad, weryfikację zastosowania, przekazanie wiedzy oraz cykliczne utrzymanie. Szkolenia z PBI opierają się na zatwierdzonych zasadach; ćwiczenie wykorzystuje BCP/DRP i SZCD STI; utrzymanie przejmuje zatwierdzone wersje oraz wnioski SOC.

4.4 Obowiązki stron bezpieczeństwo i odbiór

Zamawiający zapewni dokumenty wejściowe, właścicieli procesów, uczestników oraz decyzje i zatwierdzenia. Warunkiem odbioru jest spełnienie kryteriów każdego pakietu, potwierdzone protokołem z kodami produktów, wersjami, wynikami weryfikacji i wykazem otwartych działań. Wynik uczestników i samo dostarczenie szablonów nie zastępują kryteriów wykonania usługi.

Weryfikacja dokumentacyjna BCP/DRP ani ćwiczenie tabletop nie potwierdzają rzeczywistego osiągnięcia RTO lub RPO. Utrzymanie dokumentów i organizacyjne wsparcie nie przejmują technicznej obsługi incydentów SOC.

Odbiór usługi Security Awareness potwierdza udostępnienie platformy i katalogu, kont dla 60 użytkowników i grup, wykonanie uzgodnionego harmonogramu w sześciomiesięcznym okresie, raporty po modułach i raport

końcowy oraz usunięcie danych po zakończeniu. Zakres funkcjonalny i obsługę określa 4.2; wynik zachowania użytkowników nie zastępuje dowodu wykonania usługi.

4.5 Zakończenie współpracy

Pakiet końcowy obejmuje aktualne dokumenty, historię zmian, rejestry, dowody przeglądów oraz listę otwartych spraw z właścicielami i terminami, zgodnie z 4.2. Warunki poprawek i terminy raportów pozostają określone oddzielnie w każdym pakiecie.

5 Zadanie 2 System klasy SIEM/SOAR z modułem GRC

5.1 Przedmiot cel i zakres zamówienia

Zadanie łączy zarządzanie ryzykiem z wykrywaniem i obsługą cyberzagrożeń. Rezultatem jest wdrożony system SIEM/SOAR z modułem GRC. Platforma wykorzystuje zasady zadania 1 i sygnały IDS OT oraz wspiera SOC w ochronie ciągłości działania przedsiębiorstwa.

5.2 Wymagania funkcjonalne, techniczne i realizacyjne SIEM/SOAR z modułem GRC

Wykonawca zapewni dostawę licencji, wdrożenie, konfigurację, integrację, testy, dokumentację i przekazanie wiedzy dla spójnego rozwiązania SIEM/SOAR z modułem GRC. GRC stanowi część zadania 2, powiązaną z procesami zadania 1 i obsługą incydentów, a nie pominiętą pozycję organizacyjną. Zakres rozwiązania określają wymagania funkcjonalne niniejszego OPZ; zasady oceny równoważności wynikają z dokumentacji postępowania.

Wykonawca zapewni konfigurację powiązań zasobów, usług i procesów z oceną ryzyka oraz zabezpieczeniami, wykorzystując zatwierdzone dane i metody z zadania 1. Zakres obejmuje kontekst zasobów i ich zależności, ocenę prawdopodobieństwa i skutków, macierz ryzyka oraz powiązanie ustaleń z obsługą incydentów i podatności. Parametry metody i dane wejściowe zatwierdza Zamawiający. Nie należy utożsamiać oceny technicznego ryzyka z akceptacją ryzyka przez kierownictwo.

Wykonawca przekaże opis realizacji procesów GRC: zarządzania wymaganiami, kontrolami i zgodnością, obsługi audytów, ustaleń i działań korygujących, dokumentacji, rejestrów i raportowania.

Poniższe punkty 1-121 określają wymagania SIEM i SOAR oraz funkcje powiązane. Ich numeracja ma charakter lokalny w rozdziale 5.2. Wykonawca wykaże spełnienie wymagań dokumentacją i testami określonymi w OPZ.

Wymagania ogólne

Wykonawca zapewni integracje I01-I06 po stronie platformy SIEM/SOAR z modułem GRC. Ekspert GRC współpracuje z ekspertem SZBI; inżynier SIEM z administratorami źródeł i specjalistą IDS; inżynier SOAR z kierownikiem SOC. Wyniki testów potwierdzają rezultaty określone w rozdziale 3. Stosuje się wspólne wymagania punktów 1.2-1.3.

1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację odpowiedzi na zagrożenia cybernetyczne.

2. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w pełnym zakresie funkcjonalnym w strefie odseparowanej od sieci Internet.

3.Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać minimum 75 źródeł logów liczonych jako komputery oraz serwery wykorzystywane w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

Typy i charakter źródeł określa opis środowiska w rozdziale 3. Wymagane minimum 75 źródeł określa pkt 3. Licencje obejmują funkcjonalności i integracje objęte dostawą, zgodnie z pkt 5 oraz wymaganiami wdrożenia w niniejszym punkcie; Wykonawca zapewnia uprawnienia niezbędne do ich wykonania.

4. Licencja na oferowane rozwiązanie nie może nakładać limitów w zakresie liczby przechowywanych danych, ilości przesyłanych zdarzeń (EPS) oraz liczby równocześnie zalogowanych użytkowników

5. Dostarczone rozwiązanie musi być objęte 60 miesięcznym wsparciem producenta obejmującym bezpłatne dostarczanie aktualizacji oprogramowania, aktualizacji kontekstu (m.in. parsery, reguły korelacyjne i playbooki) oraz obsługę błędów.

Wykonawca zapewni licencję wieczystą zgodnie z pkt 3-5 i 111-117. Warunki licencji muszą jednoznacznie określać uprawnienia Zamawiającego do eksploatacji, moduły GRC/SIEM/SOAR i integracje oraz dalsze używanie po zakończeniu wsparcia.

Okres 60 miesięcy wsparcia producenta rozpoczyna się w dniu podpisania protokołu odbioru końcowego systemu SIEM/SOAR.

6. Rozwiązanie musi posiadać interfejs graficzny pozwalający na zarządzanie dostępnymi online aktualizacjami oprogramowania oraz kontekstem systemu, obejmującym min. reguły korelacyjne, playbooki, parsery, integracje, prompty AI, listy referencyjne oraz profile UEBA dla użytkowników i komputerów.

7. W ramach aktywnego wsparcia rozwiązanie musi udostępniać opcję przekazywania telemetrii do producenta rozwiązania w celu monitorowania poprawności działania systemu obejmując min. poprawność działania poszczególnych komponentów systemu, analizę obciążenia procesora i pamięci oraz zapisu logów oraz zdarzeń na dyskach. W przypadku awarii usług, błędów zapisu lub przeciążeniu zasobów rozwiązanie musi umożliwiać przesłanie alertu na wskazany adres a-mail. Usługa powinna działać w trybie 24/7 (24 godziny na dobę, 7 dni w tygodniu.

8. Instalacja nowych aktualizacji musi odbywać się w pełni automatycznie udostępniając operatorowi minimum dwie opcje: „instaluj” oraz „instaluj i aktywuj” dostępne jako przyciski lub menu wyboru (np.: dodanie nowej wersji reguły wraz z automatycznym jej aktywowaniem w systemie).

9. W interfejsie systemu powinien być wbudowany automatyczny mechanizm wersjonowania, zapisujący wszystkie historyczne wersje kontekstu oraz zapewniający możliwość przywracania poprzednio używanych np.: przywrócenie starszej wersji reguły korelacyjnej bądź parsera poprzez wybór z menu podręcznego wersji która ma zostać przywrócona.

10. System musi zapewniać kontrolę dostępu do danych i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role (Role Based Access Control).

11. System musi udostępniać możliwość prezentacji aktualnego stanu bezpieczeństwa organizacji, statystyk oraz wyników działania w postaci tablic (dashboard), których wygląd i rozkład poszczególnych składowych daje się dostosować do potrzeb administratora i użytkownika.

12. System musi umożliwiać generowanie raportów zgodnie z ustalonym harmonogramem oraz ich automatyczne wysyłanie na adresy e-mail definiowalnej grupy odbiorców.

13. System musi zawierać prosty interfejs graficzny do konfiguracji powiadomień, umożliwiający definiowanie warunków oraz kanałów powiadomień, określanie grup docelowych, a także konfigurację dla nich agregacji i cykliczności.

Wymagania techniczne

14. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding, IMAPS, POP3S, MAPI.

15. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC oraz agenta do czytania plików.

16. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.

17. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG, XML, JSON, REGEX oraz listę par „klucz-wartość”, gdzie logi zawierające w treści np.: „user=tomasz” powinno tworzyć pole „user” o wartości „tomasz”.

18. Proces normalizacji logów musi zawierać globalne mechanizmy wzbogacania danych, definiowane niezależnie od konfiguracji poszczególnych parserów, które na podstawie określonych warunków bazujących na polach i ich wartościach dodają nowe pola wraz z wartościami do znormalizowanych logów.

19. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł (np.: aplikacji własnych).

20. Wszystkie logi muszą być zapisywane w postaci skompresowanej.

21. System musi posiadać możliwość automatycznego rozpoznawania źródeł logów, które są do niego przekierowane (zakładając, że posiada parser dla technologii tego źródła danych). Musi automatycznie rozpoznać typ logu i dobrać dla niego odpowiedni parser, tak aby nie była wymagana żadna aktywność ze strony administratora Systemu.

22. System musi umożliwiać, przekierowywanie logów do różnych repozytoriów w zależności od ich zawartości wykorzystując w tym celu reguły bazujące na polach zdarzeń.

23. System musi samodzielnie zarządzać retencją danych oraz umożliwiać ich automatyczną archiwizację na zewnętrzne repozytoria danych.

24. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach przed nieautoryzowaną modyfikacją oraz zapewnić operatorom mechanizmy weryfikujące ich integralność.

25. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej oraz umożliwiać ich przeszukiwanie w obu formach.

26. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych.

27. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości.

28. Interfejs wyszukiwania musi obsługiwać przeszukiwanie pełnotekstowe.

29. Interfejs wyszukiwania musi obsługiwać przeszukiwanie automatyczne w wielu repozytoriach niezależnie od ich lokalizacji bez potrzeby ich wskazywania.

30. System musi zapewniać pracę z logami w czterech trybach: widoku tabelarycznym z możliwością dostosowania wyświetlanych kolumn, widoku prezentującym listę parametrów i ich wartości, widoku surowych logów oraz interaktywnej mapie sieci z wbudowanymi funkcjami wizualizacji (przeglądarka graficzna).

31. Przeglądarka graficzna w formie interaktywnej mapy sieci powinna umożliwiać dostęp do wyszukiwania logów bezpośrednio z menu kontekstowego każdego hosta. Funkcja ta musi pozwolić na wizualizację m.in. ruchu sieciowego, aktywności procesów, modyfikacji rejestru oraz wykonanych poleceń (przykład: wizualizacja wszystkich połączeń wychodzących z hosta z uwzględnieniem stref bezpieczeństwa i systemów zabezpieczeń).

32. Przeglądarka graficzna powinna umożliwiać śledzenie komunikacji, w ramach którego analiza ruchu wychodzącego z jednego hosta do drugiego, a następnie ruchu przychodzącego i wychodzącego dla drugiego hosta i uruchamianych na nim procesów, odbywa się wyłącznie za pomocą menu kontekstowych na analizowanych hostach.

33. Z poziomu każdego obiektu mapy w przeglądarce graficznej musi być dostępne menu kontekstowe pozwalające na przejście do widoku tabelarycznego logów, z zastosowanym filtrem wynikającym z graficznego wyszukiwania.

34. Z poziomu widoku tabelarycznego poprzez menu kontekstowe na kolumnach identyfikujących hosta musi być możliwość przejścia do przeglądarki graficznej w formie interaktywnej mapy sieci.

35. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

36. Interfejs do tworzenia parserów musi mieć wbudowanego asystenta AI, który będzie umożliwiał automatyczne wygenerowanie parsera na podstawie surowego logu.

37. Przeglądarka logów musi mieć wbudowanego asystenta AI, który będzie umożliwiał interpretację dowolnego logu wyzwalanego menu kontekstowym.

38. Rozwiązanie musi posiadać możliwość instalacji agentów dla systemów Windows.

39. Pełen zakres funkcjonalności agenta musi być dostępny z poziomu centralnej konsoli zarządzania.

40. Agent powinien być w pełni kontrolowany za pośrednictwem playbooków, umożliwiając wykonywanie m.in. akcji izolacji oraz blokowania na podstawie warunków związanych z analizowanymi zdarzeniami.

41. Agent powinien umożliwiać blokowanie na poziomie jądra systemu (kernela)

42. Agent powinien obsługiwać tryb komunikacji jednostronnej, w którym nie otwiera żadnych portów, a jedynie sam inicjuje połączenia z konsolą zarządzającą.

43. Agent musi przesyłać do konsoli centralnej pełen zakres telemetrii, obejmujący m.in. połączenia sieciowe, modyfikacje rejestrów, uruchamianie procesów i komend oraz dostęp do plików, w celu korelacji danych.

44. Agent powinien umożliwiać identyfikację podatności na hoście na którym zostanie zainstalowany.

45. System musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających.

46. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa do poszczególnych technik z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń według tych technik.

47. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie.

48. Reguły korelacyjne muszą umożliwiać filtrowanie z użyciem operatora LIKE oraz dopasowywanie wzorców za pomocą wyrażeń regularnych (REGEX).

49. Reguły korelacyjne muszą uwzględniać parametry obiektów w Active Directory umożliwiając odniesienie się do takiego obiektu w korelacji, na podstawie zdarzeń nie zawierających o nim informacji, przykładem będzie ruch sieciowy odwołujący się do konta użytkownika na którym hasło nie jest wymagane.

50. Reguły korelacyjne muszą uwzględniać również parametry, które nie są bezpośrednio zawarte w zdarzeniach. Przykładem jest reguła wykrywająca ruch z internetu do serwera, który w bazie CMDB został sklasyfikowany jako zasób świadczący usługi wyłącznie w sieci lokalnej.

51. Korelacja powinna odbywać się na bieżąco, już na etapie rejestrowania danych w systemie, oraz obsługiwać tryb dynamiczny, który optymalizuje wydajność poprzez selektywną korelację reguł. Przykładowo, jeśli w logu znajduje się informacja wskazująca na zdarzenie związane z ruchem sieciowym, wtedy uruchamiają się wszystkie reguły korelacyjne dotyczące analizy ruchu sieciowego. Natomiast gdy zdarzenie dotyczy samego systemu, reguły te nie są uruchamiane w kontekście bieżącego zdarzenia.

52. Reguły korelacyjne muszą posiadać mechanizm statycznego przypisywania ich do odpowiednich źródeł logów, tak aby reguły dedykowane systemom Windows nie były uruchamiane dla źródeł przesyłających logi z systemów Linux.

53. Rozwiązanie musi być w pełni konfigurowalne, umożliwiając operatorowi wybór trybu uruchamiania korelacji (statycznego lub dynamicznego) oraz definiowanie dla niej warunków przy użyciu edytora graficznego, dla wszystkich pakietów reguł (polityk).

54. System musi posiadać wybudowany i w pełni modyfikowalny silnik do oceny punktowej na podstawie ryzyka reguły korelacyjnej (tzw. Risk Score). Ryzyko musi być obliczane osobno dla adresu źródłowego, adresu docelowego oraz zidentyfikowanego konta użytkownika domeny.

55. Interfejs do tworzenia reguł korelacyjnych musi umożliwiać generowanie dynamicznych nazw i opisów reguł. Przykładowo, reguła o nazwie „Local traffic blocked” powinna pozwalać operatorowi na skonfigurowanie sposobu wyświetlania zdarzenia pod nazwą „Blocked local traffic from 192.168.1.1 to 10.1.1.1” oraz z opisem „Blocked local traffic from IP address 192.168.1.1 in LAN Zone to IP address 10.1.1.1 in WAN Zone”.

56. Rozwiązanie musi zapewniać dedykowany interfejs do strojenia reguł korelacyjnych, umożliwiający analizę tych reguł pod kątem liczby wygenerowanych przez nie zdarzeń, liczby hostów, na których zostały wyzwolone, oraz prezentujący na wykresie ich statystyki z ostatnich miesięcy.

57. Interfejs strojenia reguł umożliwi wykluczanie poszczególnych hostów, grup hostów, kont użytkowników oraz grup domenowych oraz grup użytkowników domenowych, zarówno w regułach korelacyjnych, jak i z dalszej obsługi w module SOAR.

58. Interfejs do tworzenia reguł korelacyjnych musi zawierać asystenta AI z w pełni konfigurowalną opcją automatycznego generowania reguł na podstawie danych wejściowych, np. w oparciu o zadaną kategorię MITRE ATT&CK.

59. Przeglądarka skorelowanych zdarzeń musi zawierać asystenta AI z opcją interpretacji dowolnego zdarzenia, uruchamianą z poziomu menu kontekstowego. Sposób interpretacji musi być w pełni konfigurowalny i umożliwiać rozbudowę menu kontekstowego o nowe typy interpretacji.

60. System powinien analizować zachowania użytkowników i komputerów z wykorzystaniem uczenia maszynowego, aby tworzyć i automatycznie aktualizować modele typowych zachowań, umożliwiające wykrywanie odchyleń od normy.

61. Modele zachowań powinny być automatycznie tworzone na podstawie analizy danych historycznych dla grup użytkowników i zasobów (profili) oraz umożliwiać ich ponowne przeliczenie zarówno na żądanie, np. po dodaniu nowej reguły, jak i automatycznie, w sposób cykliczny, np. raz w miesiącu.

62. Modele zachowań musza mieć możliwość konfiguracji wyłączania z nauczania poszczególnych profili oraz reguł.

63. System musi posiadać zestaw co najmniej 20 predefiniowanych i konfigurowalnych reguł służących do automatycznego przyporządkowywania użytkowników i zasobów do odpowiednich profili nauczania. Reguły te muszą zapewniać co najmniej rozdzielenie procesu nauczania zachowań użytkowników uprzywilejowanych, nieuprzywilejowanych oraz kont serwisowych, a także oddzielenie urządzeń od serwerów i stacji roboczych.

64. Algorytmy uczenia maszynowego muszą umożliwiać automatyczną analizę i naukę z danych statystycznych, takich jak liczba i rodzaje generowanych zdarzeń oraz oceny ryzyka (scoring).

65. Algorytmy uczenia maszynowego powinny wykorzystywać las izolujący do wykrywania nietypowych i odbiegających od normy aktywności.

66. Mechanizm uczenia maszynowego powinien umożliwiać wskazanie wartości w zdarzeniach, które mają zostać wykorzystane w procesie nauczania, oraz powiązanie ich z odpowiednim warunkiem kwalifikującym. Przykładem może być wykrycie procesu uruchomionego z katalogu, z którego nigdy wcześniej nie był wykonywany.

67. Algorytm UEBA musi umożliwiać konfigurację mechanizmów odrzucania wartości skrajnych, które mogą negatywnie wpływać na wyniki procesu uczenia, oraz wykluczania z analizy i nauczania określonych profili użytkowników oraz reguł detekcyjnych.

68. Rozwiązanie musi oferować dedykowany interfejs graficzny umożliwiający weryfikację procentowego postępu procesu nauczania dla każdego aktywnego profilu, wraz z informacjami o dacie zakończenia nauki oraz liczbie używanych algorytmów. Interfejs powinien pozwalać na wejście do profilu w celu uzyskania szczegółowych danych o każdym algorytmie, takich jak nazwa, typ algorytmu, minimalna liczba próbek, liczba dni potrzebnych do zakończenia nauki oraz wartość odchylenia.

69. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować nowe zdarzenia i zapisywać je w repozytorium logów.

70. Przeglądarka zdarzeń powinna umożliwiać pracę ze skorelowanymi zdarzeniami w czterech trybach: widoku tabelarycznym z możliwością dostosowania wyświetlanych kolumn, widoku prezentującym listę parametrów i ich wartości, widoku zagregowanego dla hosta lub konta użytkownika oraz widoku graficznego, opartego na interaktywnej mapie sieci z wbudowanymi funkcjami wizualizacji (przeglądarka graficzna).

71. Widok zagregowany musi prezentować zdarzenia dotyczące hosta lub konta użytkownika na osi czasu, wraz ze statystykami obejmującymi liczbę wygenerowanych zdarzeń, liczbę zastosowanych reguł, wynik punktowy (scoring) oraz liczbę wykrytych anomalii. Widok powinien umożliwiać dynamiczne filtrowanie zdarzeń z dokładnością co najmniej do jednej godziny.

72. Przeglądarka zdarzeń musi posiadać tryb graficzny umożliwiający wizualizację zasięgu skorelowanego zdarzenia na interaktywnej mapie sieci, obejmującej strefy bezpieczeństwa, systemy zabezpieczeń oraz hosty, których dotyczy dane zdarzenie.

73. Rozwiązanie powinno umożliwiać, z poziomu każdego hosta, przejście do przeglądarki graficznej w celu wizualizacji zasięgu wszystkich reguł korelacyjnych z nim powiązanych, a także ruchu wychodzącego i przychodzącego związanego z tymi regułami.

74. Przeglądarka graficzna zdarzeń musi być w pełni interaktywna, umożliwiając wyświetlanie, poprzez menu kontekstowe powiązane z każdym hostem, szczegółowych informacji o nim. Co najmniej powinny być dostępne dane dotyczące: przetwarzanych informacji, powiązanych usług krytycznych, lokalizacji użytkowników korzystających z hosta, lokalizacji serwerów, z których korzysta, zastosowanych lokalnych zabezpieczeń, liczby wykrytych podatności i incydentów, liczby powiązanych zdarzeń oraz kont użytkowników z nim związanych.

75. Przeglądarka musi umożliwiać przełączanie trybu wyświetlania dla pojedynczego zdarzenia, pozwalając na zmianę widoku prezentującego pola zdarzenia i ich wartości na opis zdarzenia generowany automatycznie na podstawie pól występujących w danym zdarzeniu. Generowany opis powinien być w pełni konfigurowalny, z możliwością definiowania warunków wpływających na zmianę formy jego prezentacji.

76. Lista zdarzeń powiązanych z kontem użytkownika musi umożliwiać podgląd komputerów, na których odnotowano aktywność tego konta, oraz kont użytkowników powiązanych z danym komputerem.

77. System musi zapewniać widok mapujący wszystkie zdarzenia powiązane z hostami i kontami użytkowników w zadanym przedziale czasu na matrycę MITRE ATT&CK, umożliwiający ocenę stopnia jej pokrycia.

78. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.

79. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci

80. System musi posiadać możliwość wizualizacji dokumentacji w formie interaktywnej mapy sieci, obejmującej strefy bezpieczeństwa, urządzenia sieciowe oraz punkty końcowe w tym serwery i komputery.

81. Elektroniczna dokumentacja musi umożliwiać zarządzanie katalogiem usług, w tym definiowanie dla każdej z nich co najmniej następujących parametrów: ważność, typ, przetwarzane informacje, zależności i wpływ na inne usługi, cykliczność, powiązane aplikacje, porty sieciowe, usługi, odnośniki (URL) oraz mapowania na zasoby IT.

82. Interfejs interaktywnej mapy sieci musi umożliwiać definiowanie dozwolonej komunikacji sieciowej dla każdego zasobu IT określonego w elektronicznej dokumentacji oraz mapowanie tej komunikacji na usługi z katalogu usług.

83. Dokumentacja musi być generowana w sposób automatyczny na podstawie dostarczonych przez producenta reguł (min. 50), których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację sieci bez ingerencji operatora.

84. System musi umożliwiać zautomatyzowaną ocenę wpływu incydentów bezpieczeństwa IT na działalność organizacji w kontekście zagrożeń informatycznych (np. utraty wizerunku), pomiędzy dowolnymi zasobami IT, bazując na elektronicznej dokumentacji, macierzy MITRE ATT&CK oraz wykrytych podatnościach.

85. Wizualizacja oceny wpływu incydentu powinna być przedstawiona w formie macierzy ryzyka, która zestawia zasoby IT z zidentyfikowanymi zagrożeniami i dynamicznie oblicza poziom ryzyka dla każdego z nich. Ocena ta musi być aktualizowana w sposób ciągły, z uwzględnieniem zmienności środowiska IT - na przykład w przypadku pojawienia się krytycznej podatności poziom ryzyka powinien zostać odpowiednio podwyższony. Interfejs systemu powinien umożliwiać korzystanie z menu kontekstowego, które dla każdego wyliczonego zagrożenia pozwala na zaprezentowanie braków w wymaganych zabezpieczeniach, rekomendacji wdrożenia nowych środków ochrony, możliwych konsekwencji dla organizacji oraz potencjalnych źródeł zagrożeń.

86. System musi umożliwiać przeprowadzenie oceny wpływu incydentów bezpieczeństwa IT na działalność organizacji zarówno w dedykowanym interfejsie graficznym, symulującym potencjalne zagrożenia jeszcze przed ich wystąpieniem (z wyłączeniem analizy samych logów), jak i w ramach obsługi incydentów, podatności oraz w playbookach.

87. Ocena wpływu incydentów bezpieczeństwa IT na działalność organizacji musi być prekonfigurowana w oparciu o predefiniowane reguły prawdopodobieństwa, jednak powinna umożliwiać dostosowanie do wymagań organizacji za pomocą edytora reguł.

88. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów.

89. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).

90. Dane zgromadzone w bazie wskaźników kompromitacji powinny być możliwe do wykorzystania w regułach korelacyjnych i playbookach.

91. System musi zapewnić możliwość synchronizacji list referencyjnych z listami publikowanymi publicznie (np.: „Tor Exit Nodes").

92. System powinien posiadać wbudowanego asystenta AI, który wspiera operatora w obsłudze zdarzeń oraz podatności.

93. Asystent AI musi umożliwiać integrację z lokalnymi oraz publicznie dostępnymi modelami językowymi (LLM).

94. Asystent AI powinien działać kontekstowo, z możliwością przypisania odpowiednich promptów do każdego kontekstu.

95. Asystent AI powinien oferować dedykowane tryby działania, obejmujące co najmniej obsługę incydentów i podatności, analizę logów oraz zdarzeń korelacyjnych, a także tworzenie integracji i parserów.

96. Asystent AI musi być wyposażony w edytor promptów, umożliwiający ich edycję oraz tworzenie nowych.

97. Prompty powinny być wersjonowane i możliwe do pobrania z portalu producenta.

98. Asystent AI musi być dostępny w trybie ciągłym oraz dynamicznie przełączać kontekst w zależności od wykorzystywanych funkcjonalności.

99. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem przypisanego do jego obsługi operatora (min. e-mail, SMS)

100. Kwalifikacja zdarzeń powinna odbywać się na podstawie zestawu reguł, które automatycznie przypiszą zdarzenie do obsługi lub je odrzucą.

101. Kwalifikacja operatora do obsługi zdarzenia powinna odbywać się na podstawie kryteriów zdefiniowanych na poziomie zespołów obsługi i obejmować m.in.

-sposób przydzielania zdarzenia, co najmniej: do osoby najmniej obciążonej lub za pośrednictwem kierownika zespołu;

-typ zdarzenia, np.: podatność, reguła korelacyjna, zgłoszenie;

-typ zasobu, m.in.: baza danych, stacja robocza, kontroler domeny, drukarka, serwer, urządzenie;

-związane z zasobem usługi;

-przetwarzane informacje;

-przynależność zasobu do jednostki organizacyjnej;

-zdefiniowane oprogramowanie.

102. Obsługiwane zdarzenia muszą posiadać zestaw 30 predefiniowanych scenariuszy obsługi (ang. playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego.

103. System musi być zdolny do pobierania informacji z innych systemów oraz wykorzystywać je do podejmowania decyzji dotyczących dalszego przebiegu playbooka.

104. System musi być zintegrowany ze skanerem podatności oraz zapewnić obsługę tych podatności w ramach playbooków.

105. System musi umożliwiać reagowanie na zagrożenia zarówno poprzez integrację z innymi systemami zabezpieczeń, jak i bezpośrednio na zaatakowanej stacji roboczej lub serwerze, z poziomu obsługiwanego agenta.

106. W ramach dostępnych kroków zawartych w playbooku system musi umożliwiać przeszukiwanie logów historycznych, skorelowanych zdarzeń, statystyk UEBA, informacji o pokryciu matrycy MITRE ATT&CK oraz danych z bazy Threat Intelligence.

107. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

108. Playbooki powinny być uruchamiane zarówno w reakcji na określone zdarzenia, jak i w przypadku braku odpowiedzi w zadanym czasie, aby umożliwić realizację scenariuszy eskalacyjnych.

109. Playbooki powinny umożliwiać pełne sterowanie przy użyciu AI, w tym wykonywanie kolejnych kroków automatycznie na podstawie odpowiedzi uzyskanych od modelu LLM.

110. Playbooki powinny wykorzystywać wbudowany menedżer haseł umożliwiający bezpieczne przechowywanie danych niezbędnych do integracji, takich jak nazwy użytkowników, hasła oraz klucze API.

Wymagania dotyczące architektury

111. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji. Powinno jednocześnie umożliwiać wydzielanie warstw funkcjonalnych, zwanych dalej kolektorami, które powinny umożliwiać separację procesów takich jak parsowanie (normalizacja), przechowywanie logów, korelacja zdarzeń, przechowywanie zdarzeń oraz mechanizmy uczenia maszynowego.

112. Rozwiązanie musi mieć możliwość nieograniczonego skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów umożliwiając tym samym zarówno zwiększanie wydajności jak i niezawodności rozwiązania.

113. Kolektory przechowujące dane nie mogą wykorzystywać klasycznej relacyjnej bazy danych, dopuszcza się w tym celu jedynie bazy typu NoSQL lub autorskie rozwiązanie producenta.

114. Architektura rozwiązania musi wspierać konfigurację zapewniającą niezawodność poprzez możliwość zastosowania stosu kolektorów zastępczych, uruchamianych w przypadku awarii stosu podstawowego. Wszystkie kolektory, zarówno podstawowe, jak i zastępcze, muszą być zarządzane centralnie z poziomu tej samej konsoli.

115. Rozwiązanie musi posiadać mechanizm umożliwiający współpracę z zewnętrznymi systemami typu Load Balancer, który będzie weryfikował poprawność działania całego stosu kolektorów podstawowych. Mechanizm ten powinien udostępniać port monitorujący, za pomocą którego system zewnętrzny pozyska informację o awarii jednego z kolektorów i umożliwi odpowiednią reakcję. Przykładowo w przypadku Load Balancera reakcją będzie przełączenie na stos zapasowy, natomiast w przypadku systemu monitorowania - wygenerowanie alarmu.

116. W celu zapewnienia ciągłości korelacji kolektor podstawowy musi mieć możliwość synchronizacji zdarzeń z kolektorem zapasowym. W przypadku awarii kolektora podstawowego zdarzenia wygenerowane na tym kolektorze muszą zostać uwzględnione w korelacji na kolektorze zapasowym.

117. Wszystkie typy kolektorów, w tym agenci XDR, muszą mieć możliwość konfiguracji niezawodnościowej poprzez wskazanie kolektorów zapasowych, do których będą kierowane dane w przypadku awarii kolektorów podstawowych. Przykładem jest agent XDR, który w sytuacji braku komunikacji z kolektorem podstawowym automatycznie przekazuje dane do kolektora zapasowego.

Wymagania dodatkowe

118. Zamawiający wymaga, aby wraz z ofertą Wykonawca dostarczył próbkę systemu, udostępniając jego wersję demonstracyjną oraz aktualną dokumentację. Zamawiający, w terminie nie dłuższym niż cztery dni robocze, dokona weryfikacji zgodności oferowanego systemu na podstawie dostarczonej próbki i dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ.

119. Z uwagi na fakt, że z systemu będą korzystać również użytkownicy nieposługujący się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać funkcjonalność wgrywania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

120. Wykonawca zapewni w cenie zamówienia szkolenia z użytkowania i administrowania wdrożonym systemem lub systemami, każde dla 60 uczestników. Szkolenia kończą się przyznaniem certyfikatu producenta potwierdzającego te umiejętności. Dopuszcza się formę zdalną.

121. Wykonawca zapewni bezpłatny miesięczny dostęp do platformy szkoleniowej producenta, obejmującej szkolenia z zakresu użytkowania oraz administrowania wdrożonym systemem dla 60 osób. Platforma szkoleniowa będzie obejmować min. 30 gotowych ćwiczeń pozwalających na zapoznanie się z użytkowaniem i administrowaniem wdrożonym systemem.

Wdrożenie, integracje i dokumentacja

Wymagania funkcji produktu zależnych od centralnego katalogu pozostają zachowane i mogą być wykazane w środowisku demonstracyjnym lub testowym. Produkcyjne przyłączenie źródła tożsamości dotyczy wyłącznie systemu objętego zakresem integracji; samo wymaganie funkcji nie obejmuje wdrożenia nowej usługi tożsamości.

Wykonawca zintegruje SIEM/SOAR z IDS określonym w zadaniu 3 w zakresie dostawy określonym w 6.2. Integracja obejmuje odbiór alertu z identyfikatorem źródła, czasem, priorytetem i opisem oraz udostępnienie go SOC. Interfejs i mapowanie pól muszą odpowiadać dokumentacji dostarczanych wersji. Test I03 potwierdza ten sam alert po obu stronach; I06 potwierdza nadzór nad dostępnością telemetrii. Komponenty IDS i zakres dostawy określa 6.2; konfiguracja integracji obejmuje opisany powyżej przepływ I03 i nadzór I06.

Liczba 30 predefiniowanych playbooków nie określa liczby indywidualnie opracowywanych scenariuszy. Minimum 20 reguł profili i minimum 50 reguł aktualizacji dokumentacji pozostają odrębnymi wymaganiami katalogu. Konfiguracja scenariuszy obsługi musi realizować wymagane integracje i test I04 opisane w rozdziale 3.

Wykonawca zapewni analizę przedwdrożeniową, uzgodnienie architektury i licencji, instalację, przyłączenie źródeł, konfigurację kontekstu GRC i reguł, konfigurację SOAR, strojenie, testy oraz przekazanie do eksploatacji. Przedstawi podział konfiguracji między własnych specjalistów a administratorów Zamawiającego.

Wykonawca przekaże projekt wdrożenia i macierz zgodności Z2-P1 obejmujące komponenty, licencje, źródła, integracje, zasoby oraz mapowanie wymagań 1-121 i GRC na dowody. Dokumentacja powykonawcza Z2-P3 obejmuje architekturę, konfiguracje, katalog reguł i playbooków, integracje, role, instrukcje administracyjne, retencję, kopie i procedury odtworzenia. Wiedzę i materiały Z2-P4 przekazuje się zgodnie z pkt 120-121. Pakiet Z2-P5 obejmuje eksport uzgodnionych danych, konfiguracji i rejestrów, wykaz praw dostępu oraz instrukcję dalszego utrzymania.

Platforma wykorzystuje infrastrukturę Zamawiającego zgodnie z 5.4. Wymagania obsługi źródeł i funkcji określa katalog 5.2; zasoby, konfigurację przechowywania danych i warunki testów dokumentuje się w projekcie Z2-P1.

Wykonawca zapewni wykonanie konfiguracji, kontrolę zależności, testy, usuwanie niezgodności i bezpieczne przekazanie.

Wykonawca zapewni rozliczalność dostępu, ewidencję zmian i ochronę logów.

Wykonawca przekaże dane i konfiguracje w uzgodnionej użytecznej postaci, opis ograniczeń eksportu, instrukcje i dostęp niezbędny do dalszego utrzymania oraz rejestr otwartych błędów.

Wykonawca przeprowadzi testy wymagań objętych dostawą. Zapis każdego testu obejmuje wymaganie, dane testowe, warunek początkowy, oczekiwany i uzyskany wynik, dowód oraz osobę weryfikującą; kryteria oceny i zakres sprawdzeń określa 5.6.

5.3 Etapy realizacji i integracje

Etapy realizacji obejmują analizę przedwdrożeniową, uzgodnienie architektury i licencji, instalację, przyłączenie źródeł, konfigurację kontekstu GRC i reguł, konfigurację SOAR, strojenie, testy oraz przekazanie do eksploatacji, zgodnie z zakresem 5.2. Harmonogram szczegółowy określa kolejność i zależności tych etapów. Stan bazowy nie obejmuje poprzedniej platformy SIEM/SOAR.

5.4 Obowiązki stron i bezpieczeństwo

Zamawiający zapewni uzgodnioną infrastrukturę, dostęp administracyjny w niezbędnym zakresie, właścicieli źródeł i zatwierdzenie zmian.

5.5 Okres licencji i wsparcia

Model licencji i wymagania wsparcia określa punkt 5.2, w szczególności pkt 5 katalogu.

5.6 Testy i kryteria odbioru

Dowody odbioru: Z2-P1 - zatwierdzony projekt i macierz zgodności; Z2-P2 - skonfigurowana platforma i dowody testów źródeł, GRC, reguł, scenariuszy i uprawnień; Z2-P3 - dokumentacja powykonawcza; Z2-P4 - materiały, szkolenia i potwierdzenia producenta oraz dostęp zgodnie z pkt 120-121; Z2-P5 - pakiet przekazania i eksport. Zakres produktów określa 5.2.

Warunkiem odbioru jest przedstawienie pozytywnych wyników testów dla wszystkich wymagań objętych dostawą, uruchomienie określonych integracji oraz przekazanie Z2-P1-P5. Testy obejmują gromadzenie, normalizację, wyszukiwanie, korelację, retencję, uprawnienia, obsługę incydentu, automatyzację, kontekst ryzyka, eksport i wymagane zachowanie podczas awarii.

Test I04 potwierdza przejście kontrolnego zdarzenia przez detekcję, kwalifikację, scenariusz SOAR i obsługę SOC bez nieautoryzowanego działania na produkcji. Procedura próbki ofertowej z pkt 118 pozostaje odrębna od odbioru wdrożenia.

5.7 Zakończenie współpracy

Warunkiem zakończenia przekazania jest sprawdzenie odczytu eksportu i wycofanie uprawnień Wykonawcy według planu.

6 Zadanie 3 Wdrożenie IDS OT oraz dostawa jednej zapory bezpieczeństwa

Zadanie umożliwia wykrywanie zagrożeń i anomalii w sieci technologicznej z zachowaniem bezpieczeństwa procesu. Rezultatem jest uruchomiony IDS z licencjami, sondami i dokumentacją. Jego alerty zasilają SIEM i SOC oraz ocenę ryzyka dla ciągłości dostaw wody.

6.1 Przedmiot cel i zakres

Zadanie obejmuje dostawę i wdrożenie IDS z nowymi sondami, licencją komponentu zarządzającego i wsparciem w zakresie 6.2 oraz dostawę jednej zapory bezpieczeństwa do separacji IT/OT zgodnie z załącznikiem A. Zapora i pasywny IDS pełnią odrębne funkcje.

6.2 Wymagania funkcjonalne, techniczne i realizacyjne monitorowania OT

Przedmiotem zamówienia jest:

1. wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),

2. dostawa licencji komponentu zarządzającego oraz minimum 3 nowych sond sprzętowych z dedykowanymi zasilaczami, zgodnie z zakresem opisanym poniżej,

3. udzielenie wsparcia dla administratorów Zamawiającego,

4. organizacja i realizacja szkoleń produktowych dla administratorów

1. Funkcjonalność i specyfikacja.

Wykonawca zapewni integrację I03 po stronie IDS oraz nadzór nad dostępnością telemetrii I06, we współpracy specjalisty IDS z inżynierem SIEM i SOC. Wyniki testów potwierdzają rezultaty określone w rozdziale 3. Stosuje się wspólne wymagania punktów 1.2-1.3.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.

2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.

3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe - zarówno sondy fizyczne, jak i wirtualne - muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.

4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.

5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.

6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.

7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.

8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.

9. System IDS musi zapewniać:

a. pasywne monitorowanie sieci przemysłowej Zamawiającego,

b. automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.

c. szczegółową inwentaryzację urządzeń,

d. automatyczne odzwierciedlenie połączeń komunikacyjnych,

e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,

f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,

g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,

h. obsługę LLDP, CDP, CIP, SSDP.

10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.

11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.

12. System IDS musi mieć możliwość dodawania nowego typu protokołu.

13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.

14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line" przy wpięciu do linii.

15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).

16. System IDS musi monitorować i klasyfikować cyber incydenty oraz zdarzenia operacyjne.

17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.

18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.

19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)

20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.

21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.

22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.

23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.

24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.

25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.

26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.

27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.

28. System IDS musi wykrywać zagrożenia min.:

a. malware/"zero-day",

b. atak DOS/DDOS,

c. atak typu ATP,

d. spyware, skanowanie sieci,

e. zagrożenia Man-in-the-Middle,

f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,

g. wykrywanie połączeń do innej sieci LAN/internet,

h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.

29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.

30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.

31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.

32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.

33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.

34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.

35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.

36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.

37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją, w której podsieci zostały one wykryte.

38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.

39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.

Dostawa obejmuje minimum 3 nowe sondy sprzętowe do pasywnej analizy ruchu, każdą z dedykowanym zasilaczem przystosowanym do warunków infrastruktury przemysłowej, oraz oprogramowanie komponentu zarządzającego i analizującego ruch z licencją typu site, bez limitu liczby monitorowanych aktywów w objętej licencją lokalizacji. Licencja obejmuje współpracę z dostarczanymi sondami i wymagane funkcje systemu. Sondy i komponent zarządzający spełniają katalog 1-39. Wykonawca zapewni montaż, instalację i konfigurację. Dostawa nie obejmuje dodatkowej sondy zapasowej. Pasywność, sposoby pozyskania kopii ruchu, limit modelowania, protokoły i pasywny SBOM określają pkt 13-14, 17, 24-25 i 33; kryteria odbioru określa 6.7.

Wykonawca zapewni wsparcie techniczne i serwis producenta oprogramowania oraz dostarczonych sond przez 36 miesięcy od odbioru IDS, obejmujące poprawki bezpieczeństwa, aktualizacje baz sygnatur protokołów przemysłowych oraz asystę techniczną. Dopuszcza się licencję bezterminową albo terminową zapewniającą pracę systemu przez cały okres wsparcia; Wykonawca wskaże w ofercie model licencji, jej okres ważności oraz prawa do korzystania z systemu po zakończeniu wsparcia. Czasy reakcji SOC określone w rozdziale 7 nie są czasami serwisu producenta IDS.

Wykonawca zapewni rozpoznanie na podstawie dokumentacji i wizji lokalnej w uzgodnionym zakresie, projekt punktów pozyskania ruchu, dostawę i montaż, instalację systemu, konfigurację sond, uczenie, strojenie, testy i odbiór.

Wykonawca opracuje projekt i wykaz dostawy obejmujące komponenty, licencje, sondy, punkty pozyskania ruchu i zasady montażu. Dokumentacja powykonawcza obejmuje architekturę podłączenia, wykaz urządzeń i protokołów, konfiguracje i reguły, wersje, kopie oraz instrukcje obsługi, aktualizacji i odłączenia. Szkolenie administratorów i użytkowników zapewnia udział 60 uczestników i obejmuje interpretację alarmów, strojenie, eksport, aktualizację i obsługę awarii, z materiałami i potwierdzeniem udziału. Zasady organizacji grup określa rozdział 1.

Wykonawca zapewni wykonanie montażu, konfiguracji i testów w autoryzowanych oknach, udokumentowanie braku nieautoryzowanego ruchu do OT i plan wycofania. Do czasu wyboru bezpiecznej architektury nie wolno wykonywać wpięcia w linię produkcyjną.

Dostęp SOC i sposób przekazywania alertów muszą spełniać warunek lokalnego przetwarzania z pkt 2 katalogu. Eksport PCAP, list urządzeń i protokołów podlega ochronie informacji wrażliwych. Funkcje zdalnej aktualizacji sond nie uprawniają do zmiany nastaw urządzeń technologicznych.

Wykonawca przekaże konfiguracje i dostępne eksporty zgodnie z pkt 36-38, dokumentację, inwentarz licencji, listę otwartych ustaleń i plan bezpiecznego odłączenia lub przejęcia utrzymania.

Testy wykonuje się na kontrolowanym ruchu lub plikach PCAP, bez rzeczywistego ataku na produkcję.

6.3 Etapy i integracje

Kolejność etapów obejmuje rozpoznanie na podstawie dokumentacji i wizji lokalnej w uzgodnionym zakresie, projekt punktów pozyskania ruchu, dostawę i montaż, instalację systemu, konfigurację sond, uczenie, strojenie, testy i odbiór. Uczenie rozpoczyna się po uruchomieniu poprawnego odbioru kopii ruchu reprezentującego normalną pracę monitorowanej sieci; limit modelowania określa pkt 17 katalogu 6.2. Integracje I03 i I06 realizuje się zgodnie z 6.2.

6.4 Produkty dokumentacja i szkolenia

Produkt	Warunek odbioru (wymagania realizacyjne w 6.2)
Z3-P1 Projekt i wykaz dostawy	Komponent zarządzający z licencją typu site, minimum 3 nowe sondy sprzętowe z zasilaczami, punkty pozyskania ruchu oraz zatwierdzone zasady montażu, zgodnie z 6.2.
Z3-P2 IDS i integracja	Monitoring uzgodnionych segmentów, mapa aktywów i komunikacji, wykrycie bezpiecznych zdarzeń kontrolnych oraz alert w SIEM.
Z3-P3 Dokumentacja powykonawcza	Architektura podłączenia, wykaz urządzeń i protokołów, konfiguracje i reguły, wersje, kopie, instrukcje obsługi, aktualizacji i odłączenia.
Z3-P4 Przekazanie wiedzy	Szkolenie administratorów z interpretacji alarmów, strojenia, eksportu, aktualizacji i obsługi awarii wraz z materiałami i potwierdzeniem udziału.

6.5 Obowiązki stron i ochrona procesu

Zamawiający zapewni właścicieli sieci i procesu, dane o urządzeniach i protokołach, uzgodnione zasilanie i miejsca montażu oraz zatwierdzenie punktów kopii ruchu.

6.6 Licencje gwarancja utrzymanie i serwis

Zakres dostawy, licencji, 36-miesięcznego wsparcia i serwisu oraz szkoleń IDS określa 6.2. Dla jednej zapory obowiązują wymagania gwarancji, subskrypcji i wsparcia zawarte w załączniku A.

6.7 Testy i kryteria odbioru

Warunkiem odbioru jest pozytywny wynik macierzy testów wszystkich wymagań 1-39, potwierdzenie dostawy minimum 3 nowych sond z zasilaczami i komponentu zarządzającego z licencją typu site oraz zgodności dostawy z 6.2 i projektem, potwierdzenie pasywności, widoczności uzgodnionych segmentów, obsługi właściwych protokołów, integracji I03 i przekazania Z3-P1-P4. Dowód obejmuje wyniki IDS i SIEM, czasy oraz potwierdzenie właściciela OT. Niewidoczność urządzenia lub składnika oprogramowania nie może być prezentowana jako potwierdzenie jego braku.

6.8 Zakończenie współpracy

Zamawiający zatwierdzi operacje wpływające na sieć. Kryteria testów IDS określa 6.7, a zakres dokumentacji, eksportów i planu przejęcia utrzymania - 6.2; dla zapory obowiązuje A.4. Lokalny dostęp SOC musi spełniać zasady rozdziału 3 i warunek przetwarzania danych z 6.2. Terminy udostępnienia środowiska i okna wdrożenia ujmuje się w harmonogramie w granicach terminu realizacji zamówienia.

7 Zadanie 4 Usługa monitoringu SOC dla środowisk IT i OT

Zadanie zapewnia operacyjne wykrywanie, analizowanie i eskalowanie zagrożeń dla przedsiębiorstwa. Rezultatem jest uruchomiona usługa SOC obejmująca monitoring IT i OT oraz udokumentowaną obsługę incydentów. SOC wykorzystuje SIEM, SOAR i IDS OT oraz przekazuje wnioski do SZBI i działań chroniących ciągłość dostaw wody.

7.1 Przedmiot cel i zakres

Przedmiotem jest usługa SOC dla IT i OT, powiązana z zadaniami 1-3. Wymagania realizacyjne określa 7.2.

7.2 Wymagania dotyczące realizacji usługi SOC

Wykonawca zapewni obsługę integracji I04-I06 po stronie SOC, we współpracy kierownika SOC z inżynierem SOAR, ekspertem SZBI, inżynierem SIEM i specjalistą IDS. Wyniki testów potwierdzają rezultaty określone w rozdziale 3. Stosuje się wspólne wymagania punktów 1.2-1.3.

Wykonawca zapewni świadczenie usługi SOC w powiązaniu z zadaniami 1-3, przy zachowaniu poniższych minimalnych parametrów. Usługa obejmuje IT i OT zgodnie z zamkniętym katalogiem źródeł i uzgodnionym zakresem działań. Dane OT pozostają chronione warunkami zadania 3; model zdalnego dostępu nie może powodować nieuzgodnionego transferu danych.

1. Usługa SOC obejmuje:

1) Monitorowanie infrastruktury IT i OT pod kątem wykrywania i analizy zdarzeń bezpieczeństwa oraz identyfikacji nietypowych i podejrzanych aktywności.

2) Reagowanie na incydenty - klasyfikacja incydentów, analiza i weryfikacja zdarzeń oraz podejmowanie działań ograniczających ich skutki.

3) Zarządzanie podatnościami - cykliczne skany podatności oraz współpraca w zakresie eliminacji zagrożeń.

4) Raportowanie i rekomendacje prewencyjne mające na celu minimalizację ryzyka przyszłych incydentów

2. Wymagania kwalifikacyjne zespołu SOC określa rozdział 2.

3. Zakres świadczenia usługi:

1) Stały monitoring i obsługa incydentów 24/7/365.

2) Wsparcie konsultacyjne z zakresu cyberbezpieczeństwa.

3) Dostarczenie oraz utrzymanie technologii i infrastruktury niezbędnej do świadczenia usługi.

4) Bieżąca komunikacja i współpraca z zespołem bezpieczeństwa organizacji zamawiającej.

5) Raportowanie bieżące i okresowe oraz rekomendacje w zakresie poprawy bezpieczeństwa.

4. Jednostka Security Operation Center powinna spełniać w całości Rozporządzenie 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

5. 1) Pierwsza linia wsparcia (Tier 1):

a) Odpowiada za natychmiastowe przyjęcie zgłoszenia, wstępną analizę i triage incydentu.

b) Czas reakcji: natychmiast po otrzymaniu zgłoszenia lub automatycznym wykryciu przez system monitoringu do 15 min.

2) Druga linia wsparcia (Tier 2):

a) Prowadzi zaawansowaną analizę incydentu, podejmuje działania naprawcze i koordynuje reakcję eliminującą zagrożenie.

b) Czas reakcji: uruchamiana w ciągu 1 godziny od eskalacji przez pierwszą linię.

3) Trzecia linia wsparcia (Tier 3):

a) Czas reakcji: podejmuje działania w ciągu 4 godzin od eskalacji incydentu przez drugą linię; w przypadku skomplikowanych zdarzeń, prace uruchamiane są natychmiast po potwierdzeniu potrzeby przez Tier 2, z gwarancją rozpoczęcia działań do 4 godzin.

Wykonawca zapewni przygotowanie planu uruchomienia, potwierdzenie źródeł, dostępów, personelu, kanałów kontaktu, zasad klasyfikacji i eskalacji, a następnie testy przepływu i przekazanie do obsługi. Wykonawca przekaże wykaz zależności między utrzymaniem technologii SOC a dostawami zadań 2 i 3, aby te same komponenty nie były rozliczane podwójnie.

Wykonawca zapewni rejestrację wykrycia lub zgłoszenia, wstępną analizę, kwalifikację, przydział, eskalację i historię działań. Priorytet uwzględnia wpływ na ludzi, proces, dostawy wody, zasoby i informacje. Reakcja SOC nie przenosi na Wykonawcę uprawnień do sterowania procesem technologicznym.

Wykonawca zapewni zapis znaczników wykrycia, rejestracji, podjęcia i eskalacji pozwalający obliczyć uzgodnione czasy.

Wykonawca zapewni obsługę braku telemetrii jako odrębnego problemu widoczności, ze wskazaniem niedostępnego źródła, początku przerwy, wpływu i podjętych działań. Brak alertów nie może być raportowany jako brak zagrożeń przy niedostępnych danych. Sposób wykrycia i próg alarmowania określa rejestr integracji I06.

Wykonawca przekaże raporty bieżące o incydentach oraz okresowe raporty operacyjne i zarządcze obejmujące pokrycie źródeł, przerwy telemetrii, liczbę i priorytety zgłoszeń, czasy obsługi, naruszenia SLA, podatności, rekomendacje i otwarte działania. Ustalenia przekazywane do SZBI i GRC muszą zawierać identyfikator, kontekst zasobu, właściciela i stan obsługi.

Wykonawca zapewni personel, utrzymanie usługi, monitoring, analizę, eskalację i wsparcie incydentów w wymaganym zakresie. Wykonawca zapewni zatwierdzany zakres skanów podatności, okna, wyłączenia OT i warunki przerwania. Cykliczne skany określone w pkt 1 nie uprawniają do aktywnego badania urządzeń OT bez zgody.

Wykonawca zapewni konta imienne, minimalne uprawnienia, kontrolowany dostęp zdalny i uprzywilejowany, rejestr działań i ochronę materiału incydentowego. Wykonawca przekaże instrukcję współpracy i eskalacji oraz przeprowadzi przekazanie wiedzy osobom Zamawiającego.

Wykonawca zapewni kontrolowane przekazanie otwartych incydentów, historii, reguł i konfiguracji należących do Zamawiającego, zachowanie wymaganej retencji oraz uzgodnioną pomoc przy przejęciu. Wykonawca przekaże potwierdzenie usunięcia własnych dostępów i zwrotu lub usunięcia kopii roboczych.

7.3 Uruchomienie i integracje

Uruchomienie obejmuje przygotowanie, testy przepływu i przekazanie do obsługi zgodnie z 7.2. Obowiązki dotyczące technologii i infrastruktury niezbędnej do świadczenia usługi określa pkt 3 punktu 7.2, z uwzględnieniem dostaw zadań 2 i 3 i zakazu podwójnego rozliczania tych samych komponentów.

7.4 Obsługa incydentów i pomiar czasów

Zamawiający zapewni osoby uprawnione do autoryzacji izolacji, zmian, odtworzenia i komunikacji zewnętrznej.

Pomiar czasów odnosi się do SLA określonego w pkt 5 punktu 7.2. Nie utożsamia się czasu reakcji z czasem rozwiązania incydentu.

7.5 Telemetria raportowanie i współpraca

Produktami są bieżące raporty incydentowe oraz okresowe raporty operacyjne i zarządcze, zgodnie z zakresem w 7.2.

7.6 Obowiązki bezpieczeństwo i wiedza

Zamawiający zapewni informacje o zmianach i krytyczności, udział IT, OT i eksploatacji oraz decyzje zastrzeżone dla właścicieli.

7.7 Produkty testy i kryteria odbioru

Produkt	Warunek odbioru
Z4-P1 Plan usługi i instrukcja współpracy	Zamknięty zakres, okres, źródła, role, kanały, macierz eskalacji i zatwierdzone zasady działania.

Produkt	Warunek odbioru
Z4-P2 Uruchomiony monitoring	Testowe zdarzenie IT i OT dociera do SOC, otrzymuje kwalifikację, właściciela i historię eskalacji; test I06 wykazuje przerwę telemetrii.
Z4-P3 Rejestry i raporty	Weryfikowalna historia działań i pomiarów, raporty pokrywające uzgodniony okres i źródła; odrębne wykazanie braków widoczności.
Z4-P4 Pakiet końcowy	Eksport zgłoszeń i raportów, otwarte incydenty, rekomendacje, przekazanie wiedzy oraz potwierdzone odebranie dostępów.

Odbiór uruchomienia SOC potwierdza dostarczenie Z4-P1, pozytywne wyniki testów Z4-P2, działanie podstawowego i awaryjnego kanału komunikacji, pomiary czasów oraz ochronę danych i autoryzację działań. Odbiór okresowy opiera się na wykonanej usłudze, raportach i dowodach SLA; sam brak incydentów go nie zastępuje. Niezgodności ujmuje się z określeniem wpływu, właściciela i terminu usunięcia. Plan przejścia obejmuje przekazanie określone w 7.2 i 7.8 oraz produkty Z4-P3 i Z4-P4.

7.8 Zakończenie usługi

Termin końca monitorowania i początku obsługi następcy musi być zatwierdzony, aby uniknąć luki nadzoru. Przekazanie obejmuje produkty i czynności określone w 7.2 i 7.7. Nie ustanawia się nieograniczonej bezpłatnej gotowości po zakończeniu usługi.

8 Odbiór całości i kontrola zależności

Warunkiem odbioru całości jest spełnienie kryteriów czterech zadań, w tym zakresu dostawy jednej zapory z załącznika A, potwierdzone testami I01-I06, sprawdzeniami A.4 i kompletnością dokumentacji. Wykonawca przekaże macierz wymaganie-produkt-test-dowód-wynik oraz protokół zbiorczy z wykazem wersji i otwartych działań. Zamawiający zapewni udział właścicieli biznesowych, SZBI, IT, OT i eksploatacji. Nie można uznać istotnej niespełnionej funkcji za wykonaną przez wpisanie jej do listy przyszłych działań.

Test całości wykorzystuje kontrolny alert OT, przekazanie do SIEM, uzgodnioną obsługę SOAR/SOC i odnotowanie wniosku w procesie SZBI/GRC. Weryfikuje się także zdarzenie IT oraz przerwę telemetrii. Testy nie mogą wymagać rzeczywistego zakłócenia dostaw wody.

9 Słownik pojęć

Skrót lub termin	Znaczenie
OPZ / SWZ	Opis Przedmiotu Zamówienia / Specyfikacja Warunków Zamówienia
IT / OT / STI	Technologie informatyczne / technologie operacyjne / systemy teleinformatyczne
SZBI / PBI / SZCD	System Zarządzania Bezpieczeństwem Informacji / Polityka Bezpieczeństwa Informacji / System Zarządzania Ciągłością Działania
GRC	Governance Risk and Compliance - ład organizacyjny, ryzyko i zgodność
SIEM / SOAR / SOC	Security Information and Event Management / Security Orchestration Automation and Response / Security Operations Center
IDS / ICS / IIoT	Intrusion Detection System / Industrial Control Systems / Industrial Internet of Things
BCP / DRP / BIA	Business Continuity Plan / Disaster Recovery Plan / Business Impact Analysis
RTO / RPO / SLA	Recovery Time Objective / Recovery Point Objective / Service Level Agreement
CMDB / UEBA / XDR	Configuration Management Database / User and Entity Behavior Analytics / Extended Detection and Response
AI / ML / LLM	Sztuczna inteligencja / uczenie maszynowe / duży model językowy
EPS / HA / RBAC	Zdarzenia na sekundę / wysoka dostępność / kontrola dostępu oparta na rolach
PLC / HMI / RTU / IED / SCADA	Sterownik programowalny / interfejs operatora / zdalna jednostka terminalowa / inteligentne urządzenie elektroniczne / nadzór i pozyskiwanie danych
SPAN / mirror / in-line	Kopia ruchu z przełącznika / lustrzany port / wpięcie w tor komunikacji
DPI / PCAP / SBOM	Deep Packet Inspection / Packet Capture / Software Bill of Materials
CVE / IoC / CTI	Common Vulnerabilities and Exposures / wskaźnik kompromitacji / informacje o zagrożeniach
KSC / NIS2 / RODO / PZP	Krajowy System Cyberbezpieczeństwa / dyrektywa (UE) 2022/2555 / rozporządzenie (UE) 2016/679 / Prawo zamówień publicznych
PCA / ISO / IEC / NIST	Polskie Centrum Akredytacji / International Organization for Standardization / International Electrotechnical Commission / National Institute of Standards and Technology
CISO / CSIRT / SIM3	Chief Information Security Officer / Computer Security Incident Response Team / Security Incident Management Maturity Model
CISM / CISA / CRISC	Certified Information Security Manager / Certified Information Systems Auditor / Certified in Risk and Information Systems Control
OSCP / CEH / CySA+	Offensive Security Certified Professional / Certified Ethical Hacker / Cybersecurity Analyst
ITIL / PM² / SC-200	Information Technology Infrastructure Library / metodyka zarządzania projektami Komisji Europejskiej / kod egzaminu Microsoft Security Operations Analyst

Skrót lub termin	Znaczenie
API / ODBC / TLS / NTP	Interfejs programistyczny / Open Database Connectivity / Transport Layer Security / Network Time Protocol
CEF / LEEF / URI / URL	Common Event Format / Log Event Extended Format / Uniform Resource Identifier / Uniform Resource Locator
XML / JSON / REGEX / RAW	Extensible Markup Language / JavaScript Object Notation / wyrażenie regularne / surowe dane
IMAPS / POP3S / MAPI	Zabezpieczone protokoły dostępu do poczty IMAP i POP3 / Messaging Application Programming Interface
LLDP / CDP / CIP / SSDP	Link Layer Discovery Protocol / Cisco Discovery Protocol / Common Industrial Protocol / Simple Service Discovery Protocol
DNP3 / OPC UA / TASE2	Distributed Network Protocol 3 / OPC Unified Architecture / Telecontrol Application Service Element 2
MAC / LAN / IP / SMS / CSV / PDF	Adres warstwy łącza / sieć lokalna / Internet Protocol / krótka wiadomość tekstowa / wartości rozdzielone separatorem / Portable Document Format
DoS / DDoS / APT	Odmowa usługi / rozproszona odmowa usługi / zaawansowane trwałe zagrożenie
ATP / BUSZ	Oznaczenia użyte w katalogu wymagań IDS: ATP w pkt 28 lit. c, BUSZ w pkt 25 punktu 6.2
MISP / MITRE ATT&CK / NoSQL	Platforma wymiany informacji o zagrożeniach / baza technik przeciwnika MITRE / klasa nierelacyjnych baz danych
Playbook / parser / triage	Scenariusz obsługi / reguła interpretacji danych / wstępna kwalifikacja zgłoszenia
TI / ID / UE	Trusted Introducer / identyfikator / Unia Europejska
TCP / WAN / SYSLOG	Transmission Control Protocol / sieć rozległa / standard przesyłania komunikatów dziennika
EGD / GE / SRTP	Ethernet Global Data / General Electric, oznaczenie rodziny urządzeń w źródle / Service Request Transfer Protocol w kontekście automatyki GE
OPC / UA	Historyczna nazwa OLE for Process Control, rodzina standardów komunikacji przemysłowej / Unified Architecture
IMAP / POP3	Internet Message Access Protocol / Post Office Protocol version 3
EtherCAT / BACnet	Ethernet for Control Automation Technology / Building Automation and Control Networks
MULTICAST / BORADCAST	Transmisja do grupy / źródłowa pisownia terminu broadcast, oznaczającego rozgłaszanie; pisownię zachowano w wymaganiu
LIKE / SP / Amd	Operator dopasowania wzorca / Special Publication w oznaczeniu publikacji NIST / Amendment, poprawka do normy
Modbus / Profinet / Profibus / Powerlink	Nazwy rodzin protokołów przemysłowych; wymagane warianty i zakres analizy określają pkt 24-25 katalogu w 6.2

Załącznik A. Dostawa i wdrożenie jednej zapory bezpieczeństwa

A.1 Przedmiot i zakres dostawy

Wykonawca dostarczy i wdroży w zadaniu 3 jedną nową zaporę (1 urządzenie) do separacji IT/OT, z funkcjami ochronnymi, licencjami, subskrypcjami, serwisem i pomocą wdrożeniową według A.2. Warunki wdrożenia określają A.3-A.5.

Wymagania określające możliwości produktu nie oznaczają obowiązku uruchomienia każdej funkcji w każdym segmencie sieci. Konfiguracja produkcyjna odpowiada zakresowi wdrożenia i zasadom bezpieczeństwa rozdziału 1. Możliwość budowy klastra jest cechą produktu; zamówienie obejmuje jedną zaporę bez wdrożenia HA. Obsługa usług katalogowych, chmur i SDN nie oznacza, że Zamawiający posiada wszystkie te systemy lub zamawia ich wdrożenie.

A.2 Wymagania funkcjonalne, techniczne i realizacyjne

Wymagania Ogólne

ZAP-001. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

ZAP-002. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

ZAP-003. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

ZAP-004. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

ZAP-005. System wspiera protokoły IPv4 oraz IPv6 w zakresie:

ZAP-006. Firewall.

ZAP-007. Ochrony w warstwie aplikacji.

ZAP-008. Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

ZAP-009. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

ZAP-010. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

ZAP-011. Monitoring stanu realizowanych połączeń VPN.

ZAP-012. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie

ZAP-013. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

ZAP-014. 5 portami Gigabit Ethernet RJ-45.

ZAP-015. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.

ZAP-016. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.

ZAP-017. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe

ZAP-018. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.

ZAP-019. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

ZAP-020. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps.

ZAP-021. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.

ZAP-022. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2 Gbps.

ZAP-023. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.

ZAP-024. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa

ZAP-025. W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

ZAP-026. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

ZAP-027. Kontrola Aplikacji.

ZAP-028. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.

ZAP-029. Ochrona przed malware.

ZAP-030. Ochrona przed atakami - Intrusion Prevention System.

ZAP-031. Kontrola stron WWW.

ZAP-032. Kontrola zawartości poczty - Antyspam dla protokołów SMTP.

ZAP-033. Zarządzanie pasmem (QoS, Traffic shaping).

ZAP-034. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

ZAP-035. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

ZAP-036. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.

ZAP-037. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

ZAP-038. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

ZAP-039. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

ZAP-040. Translację jeden do jeden oraz jeden do wielu.

ZAP-041. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

ZAP-042. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

ZAP-043. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.

ZAP-044. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

ZAP-045. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

ZAP-046. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

ZAP-047. Amazon Web Services (AWS).

ZAP-048. Microsoft Azure.

ZAP-049. Cisco ACI.

ZAP-050. Google Cloud Platform (GCP).

ZAP-051. OpenStack.

ZAP-052. VMware NSX.

ZAP-053. Kubernetes.

Połączenia VPN

ZAP-054. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

ZAP-055. Wsparcie dla IKE v1 oraz v2.

ZAP-056. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

ZAP-057. Obsługa protokołu Diffie-Hellman grup 19, 20.

ZAP-058. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

ZAP-059. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

ZAP-060. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

ZAP-061. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

ZAP-062. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

ZAP-063. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

ZAP-064. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

ZAP-065. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.

ZAP-066. Mechanizm „Split tunneling” dla połączeń Client-to-Site.

ZAP-067. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

ZAP-068. W zakresie routingu rozwiązanie zapewnia obsługę:

ZAP-069. Routingu statycznego.

ZAP-070. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).

ZAP-071. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

ZAP-072. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.

ZAP-073. ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu.

ZAP-074. BFD (Bidirectional Forwarding Detection).

ZAP-075. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

ZAP-076. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

ZAP-077. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

ZAP-078. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

ZAP-079. System daje możliwość określania pasma dla poszczególnych aplikacji.

ZAP-080. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.

ZAP-081. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

ZAP-082. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

ZAP-083. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

ZAP-084. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

ZAP-085. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

ZAP-086. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

ZAP-087. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

ZAP-088. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.

ZAP-089. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

ZAP-090. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

ZAP-091. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

ZAP-092. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.

ZAP-093. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

ZAP-094. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

ZAP-095. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

ZAP-096. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injection, Trojany, Exploity, Roboty).

ZAP-097. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

ZAP-098. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

ZAP-099. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

ZAP-100. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

ZAP-101. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

ZAP-102. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

ZAP-103. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.

ZAP-104. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

ZAP-105. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

ZAP-106. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

ZAP-107. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

ZAP-108. Filtr WWW dostarcza kategorii pozwalających blokować strony zgodnie z przyjętą polityką, w tym kategorii „Hazard".

ZAP-109. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.

ZAP-110. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

ZAP-111. Filtr WWW daje możliwość wykonania akcji typu „Warning" - ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

ZAP-112. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

ZAP-113. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

ZAP-114. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

ZAP-115. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

ZAP-116. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

ZAP-117. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

ZAP-118. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

ZAP-119. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.

ZAP-120. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

ZAP-121. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

ZAP-122. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

ZAP-123. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

ZAP-124. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.

ZAP-125. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

ZAP-126. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

ZAP-127. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

ZAP-128. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

ZAP-129. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

ZAP-130. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

ZAP-131. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

ZAP-132. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.

ZAP-133. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

ZAP-134. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

ZAP-135. Możliwość włączenia logowania per reguła w polityce firewall.

ZAP-136. System zapewnia możliwość logowania do serwera SYSLOG.

ZAP-137. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

ZAP-138. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

Serwisy i licencje

ZAP-139. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

ZAP-140. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

ZAP-141. Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 1 rok, na okres 60 miesięcy

Gwarancja oraz wsparcie

ZAP-142. System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Wdrożenie

ZAP-143. Zamawiający wymaga w ramach zamówienia zapewnienia pomocy wdrożeniowej realizowanej przez certyfikowanego inżyniera w następującym zakresie:

ZAP-144. - Rejestracja urządzenia / serwisów

ZAP-145. - Konfiguracja portu WAN

ZAP-146. - Konfiguracja portów LAN (maks. 5 podsieci)

ZAP-147. - Konfiguracja VLAN (maks. 5 podsieci)

ZAP-148. - Konfiguracja Profili Bezpieczeństwa (1 per moduł)

ZAP-149. - Konfiguracja Polityk Firewall (maks. 10 polityk)

ZAP-150. - Konfiguracja przekierowań portów (maks. 5 portów)

ZAP-151. - Konfiguracja VPN (Ipsec + FortiClient)

ZAP-152. - Dodanie użytkowników (maks. 5 userów)

A.3 Integracja, ochrona danych i bezpieczeństwo wdrożenia

Wykonawca skieruje logi zapory do lokalnego SIEM w ramach I02 i zapewni ich dostępność dla usługi SOC. Zakres obejmuje ruch zaakceptowany i blokowany, aktywność administratorów oraz stan urządzenia, zgodnie z wymaganiami logowania A.2. Integracja wykorzystuje obsługiwany interfejs SYSLOG z szyfrowaniem SSL/TLS. Utrata telemetrii podlega nadzorowi I06.

Wymagane w A.2 subskrypcje chmurowej analizy Sandbox oraz logowania i raportowania na 60 miesięcy, z retencją logów minimum rok, pozostają częścią dostawy. Przekazywanie danych do tych usług wymaga określenia dopuszczonego zakresu danych i przepływów zgodnie z rozdziałami 1 i 3. Dostawa licencji nie stanowi zgody na eksport danych IDS lub danych OT objętych ograniczeniami OPZ. Lokalne logowanie do SIEM nie zastępuje wymaganych licencji chmurowych.

Wdrożenie podlega wcześniejszej autoryzacji, uzgodnieniu okna zmian, ocenie wpływu i planowi wycofania zgodnie z 1.2. Dla zapory kontrolującej styk IT/OT reguły muszą odpowiadać zatwierdzonej macierzy dozwolonej komunikacji. Inspekcję, blokowanie i automatyzacje uruchamia się wyłącznie w zatwierdzonym zakresie, z zachowaniem komunikacji niezbędnej dla procesu technologicznego. Pasywny IDS pozostaje odrębnym elementem ochrony.

A.4 Produkty i kryteria odbioru

Wykonawca przekaże wykaz dostarczonych elementów i uprawnień licencyjnych, potwierdzenie rejestracji urządzenia i serwisów, okresy ważności subskrypcji i wsparcia, kopię konfiguracji oraz dokumentację wykonanych czynności wdrożeniowych. Dokumentacja i przekazanie dostępów podlegają wspólnym wymaganiom 1.3. Macierz wymaganie-produkt-test-dowód-wynik obejmuje wymagania ZAP.

Odbiór potwierdza dostarczenie jednej zapory z wymaganymi elementami, licencjami i serwisem, zgodność funkcji i parametrów z dowodami określonymi w A.2 oraz wykonanie zamówionej konfiguracji w podanych limitach. Testy obejmują uzgodnione połączenie dozwolone i blokowane, dostęp administracyjny i MFA, połączenie VPN w zamówionym zakresie, rejestrację zdarzenia w SIEM oraz wykrycie utraty telemetrii. Nie wymagają zakłócenia produkcji ani aktywnych prób na urządzeniach OT. Wyniki włącza się do protokołu odbioru całości.

A.5 Rozmieszczenie i parametry wdrożenia

Limity ZAP-143-ZAP-152 dotyczą jednej zapory i nie obejmują konfiguracji wszystkich VLAN, migracji istniejącej usługi zdalnego dostępu ani dostawy dodatkowego systemu zarządzania klientami. Subskrypcje i serwis z A.2 biegną od odbioru zapory.