Załącznik nr 8 do SWZ

Znak sprawy: ZGKiM/ZP/1/2026

Opis Przedmiotu Zamówienia

Zwiększenie odporności cybernetycznej ZGKiM Prószków

Spis treści

Opis Projektu

Celem projektu jest kompleksowe zwiększenie odporności ZGKiM Prószków na incydenty cyberbezpieczeństwa poprzez wdrożenie działań organizacyjnych, kompetencyjnych oraz technicznych, zgodnych z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz dyrektywy NIS2.

W ramach obszaru organizacyjnego zostanie opracowany, wdrożony i utrzymany System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz System Zarządzania Ciągłością Działania (SZCD), w tym plany BCP i DRP. Przeprowadzone zostaną audyty zgodności z KRI i KSC. Działania te pozwolą ustandaryzować i sformalizować procesy zarządzania ryzykiem, bezpieczeństwem i incydentami.

W obszarze kompetencyjnym planowane jest przeprowadzenie szkoleń ogólnych i specjalistycznych z zakresu cyberbezpieczeństwa, co umożliwi wzrost świadomości oraz przygotowanie kadry do skutecznego reagowania na zagrożenia.

W części technicznej IT projekt obejmuje wdrożenie systemów klasy EDR/XDR, DLP oraz SIEM, modernizację infrastruktury serwerowej i backupowej, segmenentację sieci, UTM oraz centralizację zarządzania (MDM). Dodatkowo wykonane zostanę testy podatności oraz wdrożone skanery podatności pozwalające na systemowe zarządzanie potencjalnymi lukami bezpieczeństwa.

Projekt wpisuje się w inwestycję C3.1.1 „Cyberbezpieczeństwo - CyberPL" KPO, realizując 3 cele wskazane w rozporządzeniu Ministra Cyfryzacji z 29.05.2025r.:

1. wdrożenie środków organizacyjnych dla cyberbezpieczeństwa,
2. zakup i modernizację środków technicznych,
3. rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Zasady równoważności dla sprzętu i oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Przedsiębiorstwa. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy

powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający, zgodnie z ustawą Prawo zamówień publicznych, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy (poza wyjątkami gdzie nie ma możliwości zastosowania rozwiązań równoważnych). Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy, zgodnie z art. 101 ust.4 ustawy dopuszcza rozwiązania równoważne opisywanym. Zgodnie z art. 101 ust. 5 ustawy – Zamawiający nie może odrzucić oferty tylko dlatego, że oferowane roboty budowlane, dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

Wytyczne organizacyjne zarządzania Projektem

Projekt będzie realizowany i zarządzany zgodnie z metodyką PRINCE2® (Projects IN Controlled Environments) oraz metodyką M_o_R® (Management of Risk), w sposób zapewniający kontrolę strategiczną, operacyjną oraz skuteczne i ciągłe zarządzanie ryzykiem projektowym.

Zarządzanie projektem będzie prowadzone w oparciu o podejście procesowe PRINCE2®, obejmujące w szczególności:_– przygotowanie projektu (Starting up a Project),_– inicjowanie projektu (Initiating a Project),_– strategiczne zarządzanie projektem przez Komitet Sterujący (Directing a Project),_– sterowanie etapami realizacji (Controlling a Stage),_– zarządzanie wytwarzaniem produktów (Managing Product Delivery),_– zarządzanie zakresem i jakością na poziomie etapu,_– bieżące monitorowanie postępów przy użyciu mechanizmów tolerancji,_– formalne zamykanie projektu (Closing a Project).

W ramach realizacji projektu stosowane będą mechanizmy zarządzania jakością, zarządzania zmianą oraz raportowania postępu zgodnie z zasadami i praktykami metodyki PRINCE2®, zapewniające przejrzystość działań, jednoznaczny podział ról i odpowiedzialności oraz kontrolę terminową i budżetową projektu.

Równolegle projekt będzie objęty systemowym zarządzaniem ryzykiem zgodnie z metodyką M_o_R®, obejmującym:_– określenie kontekstu ryzyka oraz warunków efektywnego zarządzania ryzykiem,_– opracowanie i stosowanie polityki oraz strategii zarządzania ryzykiem projektowym,_– identyfikację, analizę i ocenę ryzyk projektowych, w tym ryzyk kontraktowych, technicznych i finansowych,_– planowanie i wdrażanie reakcji na ryzyka,_– bieżące monitorowanie i kontrolę ryzyk oraz ocenę skuteczności działań zaradczych,_– raportowanie ryzyka na potrzeby zarządzania projektowego i decyzyjnego.

W związku z planowanym wdrożeniem rozwiązań w obszarze cyberbezpieczeństwa, Zamawiający wymaga, aby wszystkie wdrażane systemy, usługi oraz procesy były zgodne z dobrymi praktykami zarządzania usługami IT opartymi na metodyce ITIL.

Zastosowanie standardów ITIL wynika z konieczności zapewnienia:

- uporządkowanego i powtarzalnego modelu zarządzania usługami IT,

- jednoznacznego zdefiniowania procesów operacyjnych, takich jak zarządzanie incydentami, problemami, zmianą, konfiguracją oraz ciągłością działania,
- wysokiej jakości świadczenia usług oraz ich zgodności z wymaganiami organizacyjnymi i prawnymi (m.in. uoKSC, NIS2),
- efektywnej integracji wdrażanych rozwiązań z istniejącą infrastrukturą i procesami Zamawiającego.

Wdrożenie systemów cyberbezpieczeństwa bez zastosowania ustandaryzowanego podejścia do zarządzania usługami IT prowadzi do powstawania rozwiązań niespójnych, trudnych w utrzymaniu oraz podatnych na błędy organizacyjne, co w konsekwencji może negatywnie wpływać na poziom bezpieczeństwa oraz ciągłość działania organizacji.

Z uwagi na złożoność projektu, obejmującego integrację wielu systemów (m.in. SIEM, EDR, systemy backupu, rozwiązania sieciowe), konieczne jest zapewnienie spójnego modelu zarządzania ich cyklem życia – od wdrożenia, przez eksploatację, aż po rozwój i utrzymanie. Metodyka ITIL stanowi w tym zakresie uznany standard rynkowy, umożliwiający skuteczne zarządzanie usługami IT w organizacjach o podwyższonych wymaganiach w zakresie dostępności i bezpieczeństwa.

Zamawiający wymaga, aby osoba kierujące projektem posiadała kompetencje do:

- właściwego zaprojektowania procesów zarządzania usługami IT w sposób kompleksowy i zgodny z najlepszymi praktykami,
- zdolności do integracji różnych obszarów zarządzania usługami (strategia, projektowanie, wdrożenie, eksploatacja i ciągłe doskonalenie),
- odpowiedniego dostosowania metodyki ITIL do specyfiki środowiska Zamawiającego, w tym infrastruktury krytycznej oraz systemów OT,
- minimalizacji ryzyka błędów projektowych i wdrożeniowych.

Wprowadzenie powyższego wymogu jest zatem uzasadnione charakterem projektu, jego skalą oraz koniecznością zapewnienia trwałości i efektywności wdrażanych rozwiązań w całym cyklu ich życia.

Opracowanie, wdrożenie, przegląd i aktualizacja SZBI, BCP/DRP, SZCD

Celem zadania jest podniesienie poziomu dojrzałości organizacyjnej i operacyjnej Zamawiającego w zakresie cyberbezpieczeństwa, zapewnienia ciągłości działania oraz zgodności regulacyjnej, z uwzględnieniem specyfiki przedsiębiorstwa wodociągowo-kanalizacyjnego.

Realizacja zamówienia ma doprowadzić do uzyskania przez Zamawiającego kompletnej, spójnej, praktycznej i możliwej do utrzymania dokumentacji zarządczej oraz audytowej, nadającej się do stosowania operacyjnego, przeglądów kierownictwa, testowania, aktualizacji i wykazywania zgodności podczas kontroli lub audytów zewnętrznych.
Przedmiotem zamówienia jest świadczenie przez Wykonawcę usług eksperckich, doradczych, wdrożeniowych na rzecz Zamawiającego, obejmujących przygotowanie, wdrożenie, przegląd, aktualizację oraz ocenę zgodności rozwiązań organizacyjnych i proceduralnych w obszarze cyberbezpieczeństwa, ciągłości działania oraz bezpieczeństwa informacji, w szczególności w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Systemu Zarządzania Ciągłością Działania (SZCD), planów ciągłości działania (BCP), planów odtwarzania po awarii (DRP).

Zakres wsparcia przewidziany w przedsięwzięciach realizowanych w ramach programu „Cyberbezpieczne Wodociągi" obejmuje między innymi komponenty organizacyjne związane z opracowaniem, wdrożeniem, utrzymaniem i aktualizacją SZBI, SZCD, analizą ryzyka obok inwestycji w obszarze technicznym IT.

Wykonawca zobowiązany będzie do realizacji prac z należytą starannością, zgodnie z aktualnym stanem wiedzy, obowiązującymi przepisami prawa, wymaganiami normatywnymi oraz dobrymi praktykami bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania.

Wykonawca zobowiązany będzie w szczególności do:

- przeprowadzenia analizy stanu istniejącego,
- uzgodnienia z Zamawiającym harmonogramu prac,
- prowadzenia konsultacji roboczych z przedstawicielami Zamawiającego,
- uwzględnienia specyfiki organizacyjnej, procesowej i technicznej Zamawiającego,
- opracowania dokumentacji w sposób praktyczny, spójny i możliwy do stosowania,
- przekazania wszystkich produktów w formie edytowalnej oraz w formacie PDF,

- przedstawienia raportu końcowego dla każdego zadania lub etapu,
- uwzględnienia środowisk IT.

Dokumentacja opracowana przez Wykonawcę musi być przygotowana w języku polskim, z zastosowaniem terminologii urzędowej i technicznej adekwatnej do charakteru zamówienia. Zamawiający wymaga, aby wszystkie produkty posiadały jednoznaczną strukturę, wersjonowanie, datę sporządzenia, oznaczenie autora oraz wykaz zmian w przypadku aktualizacji.

Przygotowana i zatwierdzona dokumentacja musi być opublikowana na dostarczonym przez Wykonawcę portalu www umieszczonym w intranecie. Dostęp do portalu musi być limitowany do wybranych użytkowników (lub grup użytkowników) i możliwy do ustalenia atomowo do każdego dokumentu. Portal musi weryfikować uprawnienia oraz rejestrować i logować wszystkie operacje CRUD.

Aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Przedmiotem zadania jest opracowanie, wdrożenie, przegląd oraz aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji u Zamawiającego, obejmującego obszary organizacyjne, procesowe, proceduralne i dokumentacyjne, a także relacje z infrastrukturą techniczną wykorzystywaną do realizacji usług.

W ramach zadania Wykonawca zobowiązany będzie co najmniej do:

- identyfikacji kontekstu organizacji oraz stron zainteresowanych,
- identyfikacji procesów, aktywów informacyjnych, właścicieli aktywów oraz zależności,
- opracowania lub aktualizacji polityki bezpieczeństwa informacji oraz dokumentów podrzędnych,
- opracowania lub aktualizacji metodyki analizy i oceny ryzyka,
- przeprowadzenia analizy ryzyka i przedstawienia planu postępowania z ryzykiem,
- określenia ról, odpowiedzialności i zasad nadzoru nad SZBI,
- wsparcia wdrożeniowego w zakresie przyjęcia dokumentacji do stosowania,
- przeprowadzenia przeglądu wdrożonego SZBI i aktualizacji dokumentacji.

W wyniku realizacji zadania Wykonawca przekaże co najmniej:

- politykę bezpieczeństwa informacji,

- zestaw procedur, instrukcji i regulaminów niezbędnych do funkcjonowania SZBI,
- rejestr aktywów lub równoważne zestawienie aktywów objętych systemem,
- metodykę analizy ryzyka,
- raport z analizy ryzyka,
- plan postępowania z ryzykiem,
- raport z wdrożenia oraz raport z przeglądu i aktualizacji SZBI.

Za wykonane prawidłowo uznaje się zadanie, jeżeli:

- dokumentacja jest kompletna, spójna i wzajemnie niesprzeczna,
- dokumentacja została dostosowana do realiów organizacyjnych Zamawiającego,
- analiza ryzyka obejmuje uzasadnione scenariusze zagrożeń oraz proponowane sposoby postępowania,
- dokumentacja może zostać formalnie przyjęta do stosowania przez Zamawiającego,
- Wykonawca przeprowadził omówienie dokumentacji z przedstawicielami Zamawiającego.

Opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP)

Przedmiotem zadania jest opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych i zasobów wspierających działalność Zamawiającego.

W ramach zadania Wykonawca zobowiązany będzie co najmniej do:

- identyfikacji procesów krytycznych oraz usług wspieranych przez STI,
- określenia zależności pomiędzy procesami, systemami, personelem, lokalizacjami i dostawcami,
- określenia parametrów odtworzeniowych, w tym RTO i RPO, w uzgodnieniu z Zamawiającym,
- opracowania scenariuszy zakłóceń, awarii i niedostępności,
- opracowania procedur utrzymania działania w sytuacjach zakłóceń,
- opracowania procedur odtworzenia systemów i usług po awarii,
- wskazania odpowiedzialności, ścieżek eskalacji i zasad komunikacji kryzysowej,
- przygotowania scenariusza testu lub warsztatu walidacyjnego.

W wyniku realizacji zadania Wykonawca przekaże co najmniej:

- plan lub plany BCP,
- plan lub plany DRP,
- zestawienie założeń przyjętych do planowania ciągłości działania,
- macierz zależności i priorytetów odtworzeniowych,
- scenariusz testu,
- raport z testu wraz z rekomendacjami działań doskonalących.

Za wykonane prawidłowo uznaje się zadanie, jeżeli:

- plany zawierają jednoznaczne procedury działania dla określonych scenariuszy,
- plany określają role, odpowiedzialności i ścieżki komunikacji,
- plany umożliwiają zastosowanie operacyjne przez personel Zamawiającego,
- przeprowadzono uzgodnioną formę walidacji planów,
- raport z testu zawiera wnioski i działania korygujące.

Opracowanie, utrzymanie i doskonalenie Systemu Zarządzania Ciągłością Działania (SZCD)

Przedmiotem zadania jest opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Ciągłością Działania (w tym doskonalenie), obejmującego ramy zarządcze, odpowiedzialności, zasady utrzymania gotowości, testowania oraz doskonalenia zdolności organizacji do działania w sytuacjach zakłóceń.

W ramach zadania Wykonawca zobowiązany będzie co najmniej do:

- identyfikacji kontekstu działania Zamawiającego w obszarze ciągłości działania,
- opracowania lub aktualizacji polityki ciągłości działania,
- przeprowadzenia lub aktualizacji analizy wpływu na działalność (BIA) oraz identyfikacji zależności,
- określenia mechanizmów zarządczych, organizacyjnych i decyzyjnych w ramach SZCD,
- powiązania SZCD z planami BCP i DRP,
- opracowania zasad testowania, przeglądu i aktualizacji SZCD,
- wsparcia we wdrożeniu i formalizacji dokumentacji,
- przeprowadzenia przeglądu końcowego i ewentualnej aktualizacji systemu.

W wyniku realizacji zadania Wykonawca przekaże co najmniej:

- politykę ciągłości działania,
- dokument opisujący strukturę SZCD,
- wyniki BIA lub ich aktualizację,
- zestaw procedur i zasad utrzymania ciągłości działania,
- plan przeglądów i testów,
- raport z wdrożenia oraz raport z przeglądu i aktualizacji SZCD.

Za wykonane prawidłowo uznaje się zadanie, jeżeli:

- SZCD obejmuje procesy istotne dla działalności Zamawiającego,
- dokumentacja SZCD pozostaje spójna z BCP i DRP,
- określono mechanizm przeglądu, testowania i doskonalenia,
- rozwiązania są adekwatne do skali i charakteru działalności Zamawiającego,
- dokumentacja może zostać formalnie wdrożona do stosowania.

Dostawa oraz instalacja sprzętu i oprogramowania systemowego

Szafa serwerowa RACK

Parametr	Wartość
Typ szafy	Szafa serwerowa stojąca RACK
Wysokość użytkowa	48U
Standard montażowy	19”
Głębokość	min. 1200 mm
Szerokość	600 mm lub 800 mm
Nośność statyczna	min. 800 kg
Nośność dynamiczna	min. 500 kg
Konstrukcja	Spawana lub skręcana, stabilna konstrukcja stalowa
Drzwi przednie	Perforowane (min. 70% perforacji), zamykane na klucz
Drzwi tylne	Perforowane (min. 70% perforacji), dwuskrzydłowe lub jednoskrzydłowe
Panele boczne	Zdejmowane, zamykane na klucz
Szyny montażowe	Regulowane w zakresie głębokości, oznaczenie U
Wentylacja	Możliwość montażu paneli wentylacyjnych / wentylatorów
Otwory kablowe	W dachu i podłodze, z przepustami szczotkowymi lub zaślepkami
Uziemienie	Szafa wyposażona w punkt uziemienia
Stopki poziomujące	Tak
Kółka transportowe	Tak (z możliwością demontażu)
Stopień ochrony	min. IP20
Kompatybilność	Przystosowana do montażu serwerów, macierzy i urządzeń sieciowych
Akcesoria w zestawie	Komplet śrub montażowych (koszyczki, śruby, podkładki)
Kolor	Czarny lub zbliżony (RAL 9005 lub równoważny)
Normy	Zgodność z normami IEC 60297 / EIA-310

Urządzenie NAS

Parametr	Wartość wymagania
Typ urządzenia	Sieciowa macierz dyskowa / serwer NAS przeznaczony do montażu w szafie RACK
Obudowa	Obudowa RACK o wysokości maksymalnie 2U
Liczba zatok dyskowych	Minimum 12 zatok dyskowych 3,5”
Obsługiwane dyski	Obsługa dysków twardych 3,5” SATA oraz dysków SSD 2,5” SATA
Interfejs dysków	SATA 6 Gb/s oraz SATA 3 Gb/s
Wymiana dysków podczas pracy	Urządzenie musi obsługiwać wymianę dysków podczas pracy, bez konieczności wyłączania urządzenia
Procesor	Procesor 64-bitowy x86, minimum 4-rdzeniowy i 4-wątkowy, z taktowaniem w trybie zwiększonym minimum 2,9 GHz
Sprzętowe wspomaganie szyfrowania	Urządzenie musi posiadać sprzętowe wspomaganie szyfrowania AES-NI lub równoważne
Pamięć RAM	Minimum 8 GB pamięci RAM DDR4
Maksymalna obsługiwana pamięć RAM	Minimum 16 GB RAM
Pamięć flash	Minimum 4 GB pamięci flash przeznaczonej na ochronę systemu operacyjnego / mechanizm podwójnego rozruchu
Porty sieciowe podstawowe	Minimum 2 porty Ethernet 2,5GbE RJ45, zgodne w dół z 1GbE/100MbE
Agregacja połączeń	Obsługa agregacji portów / Port Trunking lub mechanizmu równoważnego
Możliwość rozbudowy sieci	Możliwość rozbudowy o interfejsy 5GbE lub 10GbE za pomocą karty rozszerzeń
Slot rozszerzeń	Minimum 1 slot PCIe, co najmniej PCIe Gen 3 x2
Porty USB	Minimum 2 porty USB 3.2 Gen 2 10 Gb/s oraz minimum 2 porty USB 2.0
Wyjście wideo	Minimum 1 port HDMI lub równoważny port wyjścia obrazu
Wake on LAN	Obsługa funkcji Wake on LAN
Jumbo Frame	Obsługa ramek Jumbo Frame

Wskaźniki LED	Wskaźniki LED informujące co najmniej o stanie dysków, statusie urządzenia, sieci LAN, rozszerzeń oraz zasilania
Przyciski	Przycisk zasilania oraz przycisk reset
Zasilanie	Redundantne zasilacze, minimum 2 sztuki
Moc zasilaczy	Minimum 300 W każdy
Zakres napięcia zasilania	100–240 V AC
Chłodzenie	Minimum 2 wentylatory systemowe
Sygnalizacja awarii	Urządzenie musi posiadać sygnalizację dźwiękową lub równoważny mechanizm ostrzegania o zdarzeniach systemowych
Temperatura pracy	Zakres pracy co najmniej od 0°C do 40°C
Wilgotność pracy	Zakres wilgotności pracy co najmniej 5–95% bez kondensacji
System operacyjny	Urządzenie musi być dostarczone z systemem operacyjnym producenta umożliwiającym zarządzanie pamięcią masową, użytkownikami, udziałami sieciowymi, kopiami zapasowymi, usługami sieciowymi i mechanizmami ochrony danych
Zarządzanie	Zarządzanie przez interfejs webowy dostępny z poziomu przeglądarki internetowej
Obsługa RAID	Obsługa macierzy RAID co najmniej w trybach RAID 0, RAID 1, RAID 5, RAID 6 oraz RAID 10
Separacja przestrzeni dyskowych	Urządzenie musi umożliwiać utworzenie odrębnych pul, wolumenów lub udziałów dla danych produkcyjnych, kopii zapasowych, danych archiwalnych oraz przestrzeni szybkiej SSD
Liczba dysków SSD	Minimum 3 sztuki dysków SSD
Typ dysków SSD	Dyski SSD 2,5” SATA, zgodne z oferowanym urządzeniem
Przeznaczenie dysków SSD	Dyski SSD przeznaczone do zastosowań serwerowych/NAS, pracy ciągłej 24/7 lub środowisk o podwyższonej intensywności operacji wejścia/wyjścia
Pojemność dysków SSD	Minimum 1,92 TB każdy lub pojemność większa
Zgodność dysków	Dyski muszą znajdować się na liście kompatybilności producenta urządzenia albo Wykonawca musi potwierdzić ich pełną zgodność z oferowanym rozwiązaniem
Montaż dysków	Wykonawca zamontuje dyski w urządzeniu oraz skonfiguruje przestrzeń dyskową zgodnie z uzgodnionym układem RAID

Osobne pule SSD i HDD	Rozwiązanie musi umożliwiać utworzenie osobnej przestrzeni/puli dla szybkich dysków SSD oraz osobnej przestrzeni/puli dla pojemnościowych dysków HDD
Monitoring dysków	System musi umożliwiać monitorowanie stanu SMART, temperatury, błędów, żywotności SSD oraz kondycji dysków
Obsługa SSD cache	Urządzenie musi obsługiwać przyspieszenie pracy przy użyciu pamięci podręcznej SSD
Protokoły plikowe	Obsługa protokołów udostępniania plików co najmniej SMB/CIFS, NFS oraz FTP/SFTP lub równoważnych
Uwierzytelnianie użytkowników	Możliwość zarządzania użytkownikami i uprawnieniami dostępu do zasobów
Integracja katalogowa	Możliwość integracji z usługą katalogową, np. Active Directory/LDAP lub równoważną
Ochrona dostępu administracyjnego	Urządzenie musi umożliwiać ograniczenie dostępu administracyjnego, konfigurację kont i uprawnień, polityk haseł, uwierzytelniania wieloskładnikowego oraz rejestrowanie działań administracyjnych
Logowanie zdarzeń	System musi umożliwiać rejestrowanie zdarzeń administracyjnych, systemowych i bezpieczeństwa
Powiadomienia	Możliwość wysyłania powiadomień o zdarzeniach, awariach i przekroczeniach progów
Monitoring pracy	Możliwość monitorowania stanu dysków, temperatur, wentylatorów, interfejsów sieciowych, wykorzystania CPU, RAM i przestrzeni dyskowej
Monitoring stanu ochrony danych	System musi umożliwiać monitorowanie stanu wolumenów, pul dyskowych, migawek, zadań kopii zapasowych, kondycji dysków oraz generowanie powiadomień o błędach, awariach lub przekroczeniu progów bezpieczeństwa
Aktualizacje	Możliwość aktualizacji systemu operacyjnego, firmware i oprogramowania urządzenia
Dokumentacja techniczna	Wykonawca dostarczy dokumentację techniczną producenta oraz instrukcję podstawowej obsługi i administracji
Dokumentacja powykonawcza	Wykonawca przekaże dokumentację powykonawczą obejmującą opis konfiguracji urządzenia, utworzone pule/wolumeny, konfigurację RAID, konta administracyjne, zasady dostępu, polityki migawek, retencji i kopii zapasowych
Montaż	Wykonawca dostarczy urządzenie przystosowane do montażu w szafie RACK wraz z wymaganymi elementami montażowymi, jeżeli są wymagane do instalacji

Konfiguracja początkowa	Wykonawca wykona montaż, pierwsze uruchomienie, aktualizację systemu, konfigurację macierzy RAID, wolumenów, udziałów, uprawnień, alertów i podstawowych mechanizmów ochrony danych
Gwarancja producenta	Minimum 36 miesięcy gwarancji producenta

Serwer

Parametr	**Wartość**
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami.
Procesor	Minimum 1 procesor klasy x86. Procesor minimum 12-rdzeniowy. Częstotliwość bazowa minimum 2,4 GHz. TDP max. 150W Pamięć podręczna procesora minimum 30 MB L3
Liczba procesorów	Możliwość rozbudowy o dodatkowy procesor.
Pamięć operacyjna	Zainstalowane minimum 265 GB pamięci RAM DDR5 ECC Registered.

	Możliwość rozbudowy pamięci RAM do minimum 8 TB. Minimum 16 gniazd DIMM dostępnych w serwerze.
Sloty roszerzeń	Serwer wyposażony w 3 aktywne gniazda PCI-Express generacji 5 pełnej wysokości (full height), przynajmniej dwa min.x8 i jedno min. x16 Możliwość rozbudowy do 8 slotów PCI-Express przy konfiguracji dwuprocesorowej.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków typu NVMe typu Hot Swap 2,5 cala. Zainstalowane 2 dyski min. 960GB SSD oraz min. 4 dyski 2TB HDD Możliwość instalacji opcjonalnego napędu DVD
Kontroler dyskowy	Sprzętowy kontroler RAID z pamięcią cache minimum 4 GB zabezpieczoną przed utratą danych. Obsługa poziomów RAID co najmniej: 0, 1, 5, 6, 10, 50, 60. Kontroler umożliwiający podłączenie dysków SAS/SATA/NVMe
Interfejsy sieciowe	Serwer musi być wyposażony minimum 4-portową kartę GbE oraz minimum 2-portową kartę 25Gbe

	Możliwość dalszej rozbudowy o interfejsy 10/25/100 GbE.
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920 x 1200 pikseli.
Porty	Serwer powinien spełniać następujące wymagania dotyczące portów USB: • Łączna liczba portów USB: minimum 4 szt. • Porty USB na panelu przednim: minimum 1 × USB 3.2 Gen1 typu A. • Porty USB na panelu tylnym: minimum 2 × USB w technologii co najmniej 3.0 typu A. • Porty USB wewnętrzne: minimum 2 porty wewnętrzne , w tym: 1 × USB 3.2 Gen1, 1 × USB 2.0. • Wymagany dedykowany port serwisowy typu USB, umożliwiający komunikację z kartą zarządzania, pozwalający na diagnostykę serwera bez konieczności ingerencji w sieć produkcyjną. Nie dopuszcza się stosowania kart PCIe , rozgałęziaczy, przedłużaczy w celu osiągnięcia wyżej wymienionych portów. 1x VGA z tyłu obudowy Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
Zasilacz i wentylatory	2 szt., zasilacze typu Hot-plug, redundantne, każdy o mocy minimum 1000W Titanium.

Bezpieczeństwo	Czujnik otwarcia obudowy współpracujący z kartą zdalnego zarządzania. Rozwiązanie wspierane przed producenta oferowanego serwera , potwierdzone w dokumentacji technicznej producenta serwera dla oferowanego modelu serwera. Wbudowany moduł TPM 2.0. Przedni panel zabezpieczający z kluczykiem umożliwiającym zdjęcie panela.
Diagnostyka	Możliwość doposażenia serwera w wysuwany panel typu LED informujący o stanie procesorów, zasilaczy, pamięci RAM , wentylatorów.
Chłodzenie	Minimum 4 redundantne wentylatory typu hot-plug
Karta/moduł zarządzający	Serwer musi posiadać zintegrowany, dedykowany kontroler zarządzający umożliwiający co najmniej: zdalny dostęp poprzez przeglądarkę WWW, zdalne włączenie, wyłączenie i restart serwera, dostęp do konsoli tekstowej i graficznej, monitorowanie stanu podzespołów, dostęp do logów sprzętowych,

	wirtualne media (mapowanie obrazu ISO), obsługę protokołów SNMP, IPMI oraz Redfish. funkcję automatycznego odzyskiwania firmware po wykryciu uszkodzenia lub nieautoryzowanej modyfikacji, możliwość przywrócenia poprzedniej wersji firmware bez udziału systemu operacyjnego, Serwer musi posiadać sprzętowy mechanizm zabezpieczający firmware oparty o nieusuwalny element kryptograficzny zapisany w układzie scalonym serwera, umożliwiający automatyczną weryfikację integralności firmware podczas każdego uruchomienia oraz automatyczne odtworzenie poprawnej wersji firmware.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022, 2025 Red Hat Enterprise Linux (RHEL) 9 SUSE Linux Enterprise Server (SLES) 15 VMware ESXi 8.x, 9.x Oracle Linux 9 VM Essentials Wsparcie musi być potwierdzone w publicznie dostępnym dokumencie na oficjalnej stronie internetowej producenta oferowanego serwera.

Wsparcie techniczne	3-letnia gwarancja producenta serwera w trybie 9x5 w miejscu instalacji z czasem reakcji następnego dnia roboczego godzin. Obsługa serwisowa prowadzona w języku polskim.
Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Inne	Dostarczony sprzęt musi być fabrycznie nowy i musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.

Serwer do kopii zapasowych z funkcją deduplikacji danych

Parametr	Wartość wymagania
Typ urządzenia	Sieciowa macierz dyskowa / serwer NAS przeznaczony do montażu w szafie RACK
Obudowa	Obudowa RACK o wysokości maksymalnie 2U
Liczba zatok dyskowych	Minimum 12 zatok dyskowych 3,5”
Obsługiwane dyski	Obsługa dysków twardych 3,5” SATA oraz dysków SSD 2,5” SATA
Interfejs dysków	SATA 6 Gb/s oraz SATA 3 Gb/s
Wymiana dysków podczas pracy	Urządzenie musi obsługiwać wymianę dysków podczas pracy, bez konieczności wyłączania urządzenia

Procesor	Procesor 64-bitowy x86, minimum 4-rdzeniowy i 4-wątkowy, z taktowaniem w trybie zwiększonym minimum 2,9 GHz
Sprzętowe wspomaganie szyfrowania	Urządzenie musi posiadać sprzętowe wspomaganie szyfrowania AES-NI lub równoważne
Pamięć RAM	Minimum 8 GB pamięci RAM DDR4
Maksymalna obsługiwana pamięć RAM	Minimum 16 GB RAM
Pamięć flash	Minimum 4 GB pamięci flash przeznaczonej na ochronę systemu operacyjnego / mechanizm podwójnego rozruchu
Porty sieciowe podstawowe	Minimum 2 porty Ethernet 2,5GbE RJ45, zgodne w dół z 1GbE/100MbE
Agregacja połączeń	Obsługa agregacji portów / Port Trunking lub mechanizmu równoważnego
Możliwość rozbudowy sieci	Możliwość rozbudowy o interfejsy 5GbE lub 10GbE za pomocą karty rozszerzeń
Slot rozszerzeń	Minimum 1 slot PCIe, co najmniej PCIe Gen 3 x2
Porty USB	Minimum 2 porty USB 3.2 Gen 2 10 Gb/s oraz minimum 2 porty USB 2.0
Wyjście wideo	Minimum 1 port HDMI lub równoważny port wyjścia obrazu
Wake on LAN	Obsługa funkcji Wake on LAN
Jumbo Frame	Obsługa ramek Jumbo Frame
Wskaźniki LED	Wskaźniki LED informujące co najmniej o stanie dysków, statusie urządzenia, sieci LAN, rozszerzeń oraz zasilania
Przyciski	Przycisk zasilania oraz przycisk reset
Zasilanie	Redundantne zasilacze, minimum 2 sztuki
Moc zasilaczy	Minimum 300 W każdy
Zakres napięcia zasilania	100–240 V AC
Chłodzenie	Minimum 2 wentylatory systemowe
Sygnalizacja awarii	Urządzenie musi posiadać sygnalizację dźwiękową lub równoważny mechanizm ostrzegania o zdarzeniach systemowych
Temperatura pracy	Zakres pracy co najmniej od 0°C do 40°C

Wilgotność pracy	Zakres wilgotności pracy co najmniej 5–95% bez kondensacji
System operacyjny	Urządzenie musi być dostarczone z systemem operacyjnym producenta umożliwiającym zarządzanie pamięcią masową, użytkownikami, udziałami sieciowymi, kopiami zapasowymi, usługami sieciowymi i mechanizmami ochrony danych
Zarządzanie	Zarządzanie przez interfejs webowy dostępny z poziomu przeglądarki internetowej
Obsługa RAID	Obsługa macierzy RAID co najmniej w trybach RAID 0, RAID 1, RAID 5, RAID 6 oraz RAID 10
Separacja przestrzeni dyskowych	Urządzenie musi umożliwiać utworzenie odrębnych pul, wolumenów lub udziałów dla danych produkcyjnych, kopii zapasowych, danych archiwalnych oraz przestrzeni szybkiej SSD
Liczba dysków SSD	Minimum 4 sztuki dysków SSD
Typ dysków SSD	Dyski SSD 2,5” SATA, zgodne z oferowanym urządzeniem
Przeznaczenie dysków SSD	Dyski SSD przeznaczone do zastosowań serwerowych/NAS, pracy ciągłej 24/7 lub środowisk o podwyższonej intensywności operacji wejścia/wyjścia
Pojemność dysków SSD	Minimum 1,92 TB każdy lub pojemność większa
Liczba dysków HDD	Minimum 4 sztuki dysków HDD
Typ dysków HDD	Dyski twarde 3,5” SATA, zgodne z oferowanym urządzeniem
Przeznaczenie dysków HDD	Dyski HDD klasy NAS lub Enterprise, przeznaczone do pracy ciągłej 24/7
Pojemność dysków HDD	Minimum 8 TB każdy lub pojemność większa
Zgodność dysków	Dyski muszą znajdować się na liście kompatybilności producenta urządzenia albo Wykonawca musi potwierdzić ich pełną zgodność z oferowanym rozwiązaniem
Montaż dysków	Wykonawca zamontuje dyski w urządzeniu oraz skonfiguruje przestrzeń dyskową zgodnie z uzgodnionym układem RAID
Osobne pule SSD i HDD	Rozwiązanie musi umożliwiać utworzenie osobnej przestrzeni/puli dla szybkich dysków SSD oraz osobnej przestrzeni/puli dla pojemnościowych dysków HDD
Monitoring dysków	System musi umożliwiać monitorowanie stanu SMART, temperatury, błędów, żywotności SSD oraz kondycji dysków
Obsługa SSD cache	Urządzenie musi obsługiwać przyspieszenie pracy przy użyciu pamięci podręcznej SSD

Deduplikacja danych	Urządzenie musi umożliwiać stosowanie mechanizmów optymalizacji wykorzystania przestrzeni dyskowej, w tym deduplikacji danych, jeżeli funkcjonalność ta jest dostępna dla zastosowanego systemu operacyjnego, systemu plików, aplikacji backupowej lub mechanizmu wykonywania kopii zapasowych
Deduplikacja w środowisku backupowym	Rozwiązanie musi umożliwiać ograniczenie zajętości przestrzeni przeznaczonej na kopie zapasowe poprzez eliminację powtarzalnych bloków lub danych w ramach obsługiwanych mechanizmów backupu, systemu plików lub aplikacji producenta
Kompresja danych	Urządzenie musi umożliwiać zastosowanie kompresji danych lub równoważnego mechanizmu zmniejszającego zapotrzebowanie na przestrzeń dyskową, zgodnie z możliwościami zastosowanego systemu operacyjnego i systemu plików
Migawki danych	Urządzenie musi obsługiwać mechanizm migawek wolumenów, udziałów lub LUN, umożliwiający odtworzenie danych do wcześniejszego punktu w czasie
Harmonogram migawek	Rozwiązanie musi umożliwiać automatyczne tworzenie migawek według harmonogramu
Retencja migawek i kopii	Rozwiązanie musi umożliwiać definiowanie okresów przechowywania migawek lub kopii danych
Ochrona przed skutkami ransomware	Urządzenie musi zapewniać mechanizmy ochrony danych przed skutkami ataków ransomware, realizowane w szczególności przez migawki, wersjonowanie, retencję kopii oraz możliwość odtworzenia danych sprzed nieautoryzowanej modyfikacji lub zaszyfrowania
Niezmienialność danych	Rozwiązanie powinno umożliwiać zastosowanie mechanizmu WORM, immutable storage lub równoważnego mechanizmu ochrony danych przed modyfikacją i usunięciem przez określony czas retencji, jeżeli jest on dostępny w zastosowanym systemie operacyjnym urządzenia
Migawki odporne na modyfikację	Rozwiązanie powinno umożliwiać zabezpieczenie migawek lub kopii danych przed przypadkowym albo nieautoryzowanym usunięciem przez określony czas retencji, zgodnie z możliwościami systemu operacyjnego urządzenia
Ochrona integralności danych	Rozwiązanie powinno zapewniać mechanizmy kontroli integralności danych na poziomie systemu plików lub wolumenów, w szczególności mechanizmy sum

	kontrolnych, wykrywania uszkodzeń danych oraz ograniczania ryzyka cichej korupcji danych, jeżeli są dostępne w zastosowanym systemie operacyjnym
Szyfrowanie danych	Urządzenie musi umożliwiać szyfrowanie danych przechowywanych na wolumenach, udziałach lub jednostkach logicznych, zgodnie z możliwościami systemu operacyjnego urządzenia
Kopie zapasowe	Obsługa tworzenia i harmonogramowania kopii zapasowych danych
Przywracanie danych po incydencie	Rozwiązanie musi umożliwiać odtworzenie danych z migawek, kopii zapasowych lub wcześniejszych wersji danych w przypadku przypadkowego usunięcia, błędu użytkownika, awarii lub incydentu ransomware
Protokoły plikowe	Obsługa protokołów udostępniania plików co najmniej SMB/CIFS, NFS oraz FTP/SFTP lub równoważnych
Uwierzytelnianie użytkowników	Możliwość zarządzania użytkownikami i uprawnieniami dostępu do zasobów
Integracja katalogowa	Możliwość integracji z usługą katalogową, np. Active Directory/LDAP lub równoważną
Ochrona dostępu administracyjnego	Urządzenie musi umożliwiać ograniczenie dostępu administracyjnego, konfigurację kont i uprawnień, polityk haseł, uwierzytelniania wieloskładnikowego oraz rejestrowanie działań administracyjnych
Logowanie zdarzeń	System musi umożliwiać rejestrowanie zdarzeń administracyjnych, systemowych i bezpieczeństwa
Powiadomienia	Możliwość wysyłania powiadomień o zdarzeniach, awariach i przekroczeniach progów
Monitoring pracy	Możliwość monitorowania stanu dysków, temperatur, wentylatorów, interfejsów sieciowych, wykorzystania CPU, RAM i przestrzeni dyskowej
Monitoring stanu ochrony danych	System musi umożliwiać monitorowanie stanu wolumenów, pul dyskowych, migawek, zadań kopii zapasowych, kondycji dysków oraz generowanie powiadomień o błędach, awariach lub przekroczeniu progów bezpieczeństwa
Aktualizacje	Możliwość aktualizacji systemu operacyjnego, firmware i oprogramowania urządzenia
Dokumentacja techniczna	Wykonawca dostarczy dokumentację techniczną producenta oraz instrukcję podstawowej obsługi i administracji

Dokumentacja powykonawcza	Wykonawca przekaże dokumentację powykonawczą obejmującą opis konfiguracji urządzenia, utworzone pule/wolumeny, konfigurację RAID, konta administracyjne, zasady dostępu, polityki migawek, retencji i kopii zapasowych
Montaż	Wykonawca dostarczy urządzenie przystosowane do montażu w szafie RACK wraz z wymaganymi elementami montażowymi, jeżeli są wymagane do instalacji
Konfiguracja początkowa	Wykonawca wykona montaż, pierwsze uruchomienie, aktualizację systemu, konfigurację macierzy RAID, wolumenów, udziałów, uprawnień, alertów i podstawowych mechanizmów ochrony danych
Gwarancja producenta	Minimum 36 miesięcy gwarancji producenta

Zarządzalny przełącznik sieciowy

Parametr	**Wartość**
Obudowa	RACK
Typ przełącznika	Zarządzalny
Przełącznik wielowarstwowy	L2/L3
Liczba portów	48x Gigabit Ethernet (10/100/1000) 4x SFP+
Przepustowość przełączania	Min. 170 GBit/s
Przepustowość	Min. 130 Mpps
Wielkość tabeli adresów	16000 wejścia
Pamięc bufora pakietów	1,5 MB
Procesor	Min. 800 MHz
Pamięć wewnętrzna	Min. 512 MB
Pamięć flash	Min. 256 MB
Dodatkowe funkcje	Obsługa QoS Zarządzanie przez www

	Agregator połączenia Obsługa VLAN Pełny dupleks Dublowanie portów IGMP snooping
Gwarancja	Minimum 24 miesiące

UTM z IDS/IPS oraz ochroną przed DDoS

Cecha	Wymagania minimalne
Parametry sprzętowe	Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
	Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
	Liczba portów Ethernet 2,5Gbps – min. 8. Liczba portów światłowodowych 1Gbps – min. 1.
	Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps
	Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps
	Przepustowość filtrowania Antywirusowego – minimum 500Mbps
	Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps
	Liczba tuneli VPN IPSec – minimum 100.
	Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
	Obsługa interfejsów 802.11q (VLAN) – minimum 128
	Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
	Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
	Liczba reguł filtrowania – minimum 8 192.
	Liczba tras statycznego routingu – minimum 512.

	Liczba tras dynamicznego routingu – minimum 10 000.
	Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
	Urządzenie musi być wyposażone w moduł TPM.
Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora sieciowa	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
	Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
	Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
	Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
	Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
	Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
	Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

	Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
	Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
	Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
	System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
IPS	System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
	Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
	Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
	Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
	Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
	Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
	Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
	Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

	Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma	Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
	Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
	Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
	Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).
	Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
	Skaner antywirusowy ma pochodzić od europejskiego producenta.
	Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
	Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
	Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL,

	c. Skaner heurystyczny.
	W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
	Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne	Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
	Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN.
	SSL VPN ma działać w trybie tunelu.
	Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
	Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal).
	Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
	Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
	Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtrowanie ruchu www	Urządzenie ma posiadać wbudowany filtr URL.
	Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
	Administrator ma mieć możliwość dodawania własnych kategorii URL.
	Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

	a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
	Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
	Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
	Filtr URL musi uwzględniać komunikację po protokole HTTPS.
	Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
	Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
	Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
Uwierzytelnianie	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory.
	Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
	Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos.
	Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

	Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
	Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
	Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
	Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
	Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
	Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
Obsługa wielu ISP	Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
	Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.
	Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
	Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
	Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

	W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
	Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing	Urządzenie ma umożliwiać statyczne trasowanie pakietów.
	Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
	Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
	Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
	Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
Funkcje administracyjne	Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w języku polskim.
	Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
	Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
	Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
	Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
	Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
	Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

	Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
	Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
	Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
	Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
	Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
	System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
	Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
	Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
	Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
	Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
	Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

	Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
	Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
	System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
	System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
	System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
	System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
	System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
	Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
	Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
	Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Funkcje dodatkowe	Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
	Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
	Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

	Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
	Urządzenie ma posiadać usługę DNS Proxy.
	Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
	Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
	Urządzenie musi mieć zaimplementowane Open API.
	Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
	Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
	Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
Gwarancja i wsparcie	Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
	W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

Punkt dostępowy do sieci WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 3 sztuki

Parametr	**Wymagania minimalne**
Obsługiwane standardy	Wi-Fi 4 (802.11 a/b/g/n)

	Wi-Fi 5 (802.11 a/b/g/n/ac) Wi-Fi 6 (802.11 a/b/g/n/ac/ax) 802.3 at (PoE+) 802.1Q
Częstotliwość pracy	2,4 GHz 5 GHz
Antena	Wewnętrzna
Zabezpieczenie transmisji bezprzewodowej	WPA WPA-PSK WPA Enterprise WPA2 WPA3
Zasilanie	POE+ (dołączony zasilacz)
Zarządzanie	Dołączony kontroler sprzętowy (do całego zestawu)
Gwarancja	12 miesięcy

Dostawa, instalacja, konfiguracja oraz parametryzacja oprogramowania

Sieciowy skaner podatności wraz z wykonaniem audytu cyberbezpieczeństwa sieci

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie systemu do skanowania podatności infrastruktury IT Zamawiającego. Rozwiązanie ma umożliwiać cykliczne i doraźne wykonywanie skanów podatności zasobów informatycznych, w tym serwerów, stacji roboczych, urządzeń sieciowych, usług sieciowych, systemów operacyjnych oraz innych zasobów wskazanych przez Zamawiającego. System powinien wspierać identyfikację znanych podatności, błędów konfiguracyjnych, nieaktualnych wersji oprogramowania, usług narażonych na atak oraz ryzyk wynikających z ekspozycji zasobów w sieci.

Rozwiązanie powinno umożliwiać wykonywanie skanów nieuwierzytelnionych oraz uwierzytelnionych, w zależności od rodzaju badanego zasobu i dostępnych poświadczeń technicznych. Skanowanie nieuwierzytelnione powinno pozwalać na ocenę zasobu z perspektywy zewnętrznego obserwatora, natomiast skanowanie uwierzytelnione powinno umożliwiać głębszą analizę systemu po zalogowaniu, w szczególności w zakresie zainstalowanych pakietów, aktualizacji, konfiguracji systemowych i podatności możliwych do wykrycia wyłącznie z poziomu uprawnionego dostępu.

System powinien stanowić narzędzie wspierające proces zarządzania podatnościami w organizacji, obejmujący wykrywanie podatności, klasyfikację ryzyka, raportowanie wyników, priorytetyzację działań naprawczych oraz weryfikację skuteczności usunięcia wykrytych nieprawidłowości. Rozwiązanie powinno umożliwiać generowanie raportów zawierających co najmniej listę wykrytych podatności, poziom ryzyka, opis podatności, dotknięte zasoby, rekomendacje działań naprawczych oraz informacje pozwalające administratorom na podjęcie działań korygujących.

Wykonawca zobowiązany jest do przeprowadzenia testów bezpieczeństwa z wykorzystaniem dostarczonego i skonfigurowanego skanera, w zakresie uzgodnionym z Zamawiającym i obejmującym wskazane zasoby infrastruktury IT/OT, systemy, usługi sieciowe oraz urządzenia objęte wdrożeniem. Testy powinny obejmować identyfikację znanych podatności, błędów konfiguracyjnych, nieaktualnych wersji oprogramowania, otwartych usług sieciowych oraz innych nieprawidłowości mogących wpływać na poziom bezpieczeństwa środowiska Zamawiającego. Po zakończeniu testów Wykonawca przekaże Zamawiającemu raport zawierający co najmniej zakres przeprowadzonych skanowań, wykaz objętych

nimi zasobów, opis wykrytych podatności wraz z oceną ich krytyczności oraz rekomendacje działań naprawczych lub ograniczających ryzyko.

System musi spełniać przedstawione w tabeli wymagania minimalne.

Obszar	Wymaganie
Typ rozwiązania	System musi być rozwiązaniem klasy skanera podatności umożliwiającym wykrywanie znanych podatności bezpieczeństwa w zasobach IT.
Model licencyjny	Zamawiający dopuszcza zastosowanie rozwiązania open source lub bezpłatnego, pod warunkiem zapewnienia jego poprawnej instalacji, konfiguracji, aktualizacji oraz przekazania procedur utrzymaniowych.
Skanowanie podatności	System musi umożliwiać wykonywanie skanów podatności zasobów sieciowych, systemów operacyjnych, usług, aplikacji i urządzeń wskazanych przez Zamawiającego.
Skanowanie nieuwierzytelnione	System musi umożliwiać wykonywanie skanów nieuwierzytelnionych, pozwalających na ocenę widocznych usług i podatności z perspektywy użytkownika bez dostępu administracyjnego.
Skanowanie uwierzytelnione	System musi umożliwiać wykonywanie skanów uwierzytelnionych z wykorzystaniem poświadczeń technicznych, w szczególności dla systemów Linux/Unix oraz Windows, jeżeli zostaną wskazane przez Zamawiającego.
Obsługa protokołów	System powinien umożliwiać analizę zasobów z wykorzystaniem standardowych protokołów sieciowych oraz usług powszechnie wykorzystywanych w infrastrukturze IT.
Profile skanowania	System musi umożliwiać definiowanie różnych profili skanowania, np. skan szybki, skan pełny, skan wybranych portów, skan wybranej grupy hostów lub skan z użyciem poświadczeń.
Zakresy skanowania	System musi umożliwiać definiowanie zakresów skanowania w oparciu o adresy IP, nazwy hostów, podsieci, grupy zasobów lub inne identyfikatory obsługiwane przez rozwiązanie.
Zarządzanie zadaniami	System musi umożliwiać tworzenie, edycję, uruchamianie, zatrzymywanie i ponawianie zadań skanowania.

Harmonogramowanie	System powinien umożliwiać planowanie cyklicznych skanów lub, jeżeli funkcjonalność harmonogramowania nie jest dostępna w wybranej wersji rozwiązania, Wykonawca musi zapewnić procedurę uruchamiania skanów cyklicznych z wykorzystaniem dostępnych mechanizmów systemowych.
Aktualizacja testów podatności	System musi umożliwiać aktualizację bazy testów podatności.
Klasyfikacja podatności	System musi klasyfikować wykryte podatności według poziomu ryzyka lub ważności, w sposób umożliwiający priorytetyzację działań naprawczych.
Opis podatności	System musi prezentować opis wykrytej podatności, podatny zasób, usługę lub komponent, poziom ryzyka oraz rekomendowane działania naprawcze.
Raportowanie	System musi umożliwiać generowanie raportów ze skanowania w formacie umożliwiającym ich analizę, archiwizację i przekazanie administratorom odpowiedzialnym za usunięcie podatności.
Historia skanów	System musi umożliwiać przechowywanie historii wykonanych skanów oraz porównywanie wyników w czasie w zakresie dostępnym w zastosowanym rozwiązaniu.
Filtrowanie wyników	System musi umożliwiać filtrowanie wyników według co najmniej zasobu, poziomu ryzyka, typu podatności, statusu oraz daty skanu.
Obsługa wyjątków	System powinien umożliwiać oznaczanie podatności jako zaakceptowane ryzyko, wynik fałszywie dodatni lub podatność do późniejszej weryfikacji, jeżeli funkcjonalność ta jest dostępna w zastosowanym rozwiązaniu.
Konta techniczne	System musi umożliwiać bezpieczne przechowywanie i użycie poświadczeń technicznych do skanów uwierzytelnionych, z ograniczeniem dostępu do tych danych wyłącznie dla uprawnionych administratorów.
Role użytkowników	System powinien umożliwiać rozdzielenie ról użytkowników, w szczególności administratora systemu, operatora skanów oraz użytkownika przeglądającego raporty.
Logowanie zdarzeń	System musi prowadzić logi zdarzeń administracyjnych, uruchamianych zadań, błędów skanowania oraz istotnych zdarzeń związanych z działaniem systemu.

Eksport danych	System powinien umożliwiać eksport wyników skanów i raportów w formatach pozwalających na dalszą analizę lub archiwizację.
Integracja	System powinien umożliwiać integrację z innymi narzędziami bezpieczeństwa lub automatyzację obsługi przez dostępne API/protokoły, jeżeli funkcjonalność ta jest dostępna w zastosowanej wersji rozwiązania.
Bezpieczeństwo dostępu	Dostęp do panelu administracyjnego systemu musi być zabezpieczony mechanizmami uwierzytelniania oraz szyfrowaną komunikacją.
Backup konfiguracji	Wykonawca musi zapewnić procedurę wykonywania kopii zapasowej konfiguracji systemu, danych skanów i raportów, w zakresie technicznie możliwym dla zastosowanego rozwiązania.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia audytu cyberbezpieczeństwa infrastruktury sieciowej Zamawiającego z wykorzystaniem dostarczonego rozwiązania skanera podatności. Audyt powinien obejmować identyfikację aktywnych zasobów sieciowych, wykrywanie znanych podatności, błędów konfiguracyjnych, nieaktualnych wersji oprogramowania, słabych punktów usług sieciowych oraz innych zagrożeń mogących wpływać na bezpieczeństwo środowiska IT. Wykonawca przeprowadzi skanowanie w sposób uzgodniony z Zamawiającym, tak aby nie zakłócić ciągłości działania systemów, a następnie opracuje raport zawierający wyniki analizy, klasyfikację wykrytych podatności według poziomu ryzyka oraz rekomendacje działań naprawczych i zabezpieczających. Wyniki audytu powinny stanowić podstawę do dalszego hardeningu infrastruktury oraz podniesienia poziomu odporności środowiska Zamawiającego na zagrożenia cyberbezpieczeństwa.

Oprogramowanie antywirusowe z modułami EDR/XDR

Przedmiotem zamówienia jest dostawa licencji oprogramowania antywirusowego z modułem EDR/XDR dla 20 użytkowników. Oprogramowania musi spełniać opisane w rozdziale wymagania funkcjonalne oraz techniczne.

Centralne zarządzanie

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku
2. polskim i angielskim.
3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania.
4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za
5. pośrednictwem protokołu szyfrowanego SSL/TLS.
6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID.
7. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
1. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
2. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego
8. producenta co konsola zarządzająca, umożliwiająca co najmniej:
    a. Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
    b. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
    c. Buforowanie ruchu HTTPS.
9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    a. Google Authenticator,
    b. Microsoft Authenticator,
    c. Authy,
    d. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

14. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
    a. Adresy sieciowe IP .
    b. Aktywne zagrożenia.
    c. Stan funkcjonowania oraz ochrony.
    d. Wersja systemu operacyjnego.
    e. Podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    a. Wyrażenie CRON.
    b. Codziennie.
    c. Cotygodniowo.
    d. Co miesiąc.
    e. Co rok.
    f. Po wystąpieniu nowego zdarzenia.
    g. Po automatycznym umieszczeniu hosta w grupie dynamicznej.
16. Rozwiązanie musi udostępniać możliwość tagowania obiektów.
17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
    a. JSON.
    b. LEEF.
    c. CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    a. Wirus.

   b. Trojan.
   c. Robak.
   d. Adware.
   e. Spyware.
   f. Dialer.
   g. Phishing.
   h. Backdoor.

4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. 7. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
   a. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
   b. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
   c. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    a. Całego dysku.
    b. Wybranych katalogów.
    c. Pojedynczych plików.
    d. Plików spakowanych oraz skompresowanych.
    e. Dysków sieciowych.

f. Dysków przenośnych.

11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    g. Wybranych plików.
    h. Wybranych procesów.
    i. Wybranych lokalizacji.
    j. Wybranych rozszerzeń.
    k. Nazwy wykrycia.
    l. Sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    a. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    b. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    c. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

A. Typ urządzenia:
    i. Pamięci masowe.
    ii. Optyczne pamięci masowe.➢ Pamięci masowe Firewire.

iii. Urządzenia do tworzenia obrazów.
iv. Drukarki USB.
v. Urządzenia Bluetooth.
vi. Czytniki kart inteligentnych.
vii. Modemy.
viii. Porty LPT/COM.
ix. Urządzenia przenośne.

B. parametry urządzenia:
i. Numer seryjny.
ii. Producent.
iii. Model.

C. typ dostępu:
i. Brak możliwości zapisu.
ii. Pełen dostęp.
iii. Ostrzeżenie użytkownika.
iv. Brak dostępu.

18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
C. Raport musi posiadać co najmniej:
    a. Listę zainstalowanych aplikacji.
    b. Listę usług systemowych.
    c. Informacje o systemie operacyjnym i sprzęcie.
    d. Listę aktywnych procesów i połączeń sieciowych.
    e. Harmonogram systemu operacyjnego.
    f. Szczegóły pliku hosts.
    g. Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
    i. Antywirus.
    ii. Zapora osobista.
    iii. Sandbox.
    iv. Antyspyware.
    v. Metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
    A. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
    B. Ochrona musi być realizowana w oparciu o co najmniej:
        i. globalna czarna lista RBL,
        ii. czarna lista użytkownika,
        iii. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres
        iv. email z książki adresowej klienta Microsoft Outlook.

23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    i. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        i. Skanowanie portów TCP oraz UDP,
        ii. Wykrywanie duplikacji adresu IP,
        iii. Atak zatruwania ARP,
        iv. Nieprawidłowa długość pakietu TCP oraz UDP.
    ii. B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        i. RDP,
        ii. SMB,
        iii. MySQL,
        iv. MSSQL.
    iii. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    B. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        i. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        iii. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
        iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
        i. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
        ii. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

iii. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
    A. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
    B. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oarciu o co najmniej:
        i. Treść komunikatu.
        ii. Obraz.

Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    i. Wirus.
    ii. Trojan.
    iii. Robak.
    iv. Adware.
    v. Spyware.
    vi. Dialer.
    vii. Phishing.
    viii. Backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi chronić pliki co najmniej za pomocą:

i. Sygnatur wirusów.
ii. Reputacji chmurowej.

7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    i. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
    ii. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    iii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    i. całego dysku,
    ii. wybranych katalogów,
    iii. pojedynczych plików,
    iv. plików spakowanych oraz skompresowanych,
    v. dysków sieciowych,
    vi. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    i. wybranych plików,
    ii. wybranych procesów,
    iii. wybranych lokalizacji,
    iv. wybranych rozszerzeń,
    v. nazwy wykrycia,
    vi. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
B. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
   i. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
   ii. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
   i. Ubuntu Desktop,
   ii. Red Hat Enterprise Linux
   iii. Linux Mint.
2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
   i. Cinnamon.
   ii. GNOME.
   iii. KDE.
   iv. MATE.
   v. XFCE.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   i. Wirus.
   ii. Trojan.
   iii. Robak.
   iv. Adware.
   v. Spyware.
   vi. Dialer.
   vii. Phishing.
   viii. Backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji.

5. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metodbjednocześnie.
6. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    i. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    ii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    i. Całego dysku.
    ii. Wybranych katalogów.
    iii. Pojedynczych plików.
    iv. Plików spakowanych oraz skompresowanych.
    v. Dysków sieciowych.
    vi. Dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    i. Wybranych plików.
    ii. Wybranych procesów.
    iii. Wybranych lokalizacji.
    iv. Wybranych rozszerzeń.
10. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    A. typ urządzenia:
        i. pamięci masowe,
        ii. optyczne pamięci masowe,
    B. B. parametry urządzenia:
        i. numer seryjny,
        ii. producent,

iii. model.

C. C. typ dostępu:

i. brak możliwości zapisu,

ii. pełen dostęp,

iii. brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   i. Microsoft Windows Server 2012 R2,
   ii. Microsoft Windows Server 2016,
   iii. Microsoft Windows Server 2019,
   iv. Microsoft Windows Server 2022,
   v. Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   i. Wirus.
   ii. Trojan.
   iii. Robak.
   iv. Adware.
   v. Spyware.
   vi. Dialer.
   vii. Phishing.
   viii. Backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    i. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    ii. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    iii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    i. całego dysku,
    ii. wybranych katalogów,
    iii. pojedynczych plików,
    iv. plików spakowanych oraz skompresowanych,
    v. dysków sieciowych,
    vi. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    i. wybranych plików,
    ii. wybranych procesów,
    iii. wybranych lokalizacji,
    iv. wybranych rozszerzeń,
    v. nazwy wykrycia,
    vi. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

C. Raport musi posiadać co najmniej:

i. Listę zainstalowanych aplikacji,

ii. Listę usług systemowych,

iii. Informacje o systemie operacyjnym i sprzęcie,

iv. Listę aktywnych procesów i połączeń sieciowych,

v. Harmonogram systemu operacyjnego,

vi. Szczegóły pliku hosts,

vii. Informacje o sterowników.

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

i. antywirus,

ii. zapora osobista

iii. sandbox,

iv. antyspyware,

v. metody heurystyczne.

15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    A. A. typ urządzenia:
        i. Pamięci masowe.
        ii. Optyczne pamięci masowe.
        iii. Pamięci masowe Firewire.
        iv. Urządzenia do tworzenia obrazów.
        v. Drukarki USB.
        vi. Urządzenia Bluetooth.
        vii. Czytniki kart inteligentnych.
        viii. Modemy.
        ix. Porty LPT/COM.
        x. Urządzenia przenośne.
    B. parametry urządzenia:
        i. Numer seryjny,
        ii. Producent,
        iii. Model.
    C. typ dostępu:
        i. Brak możliwości zapisu,
        ii. Pełen dostęp,
        iii. Ostrzeżenie użytkownika,
        iv. Brak dostępu.
18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
        i. MSSQL.
        ii. Active Directory.

iii. IIS.
iv. Sysvol.
v. DNS.
vi. DHCP .
vii. Hyper-V.
viii. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        i. Skanowanie portów TCP oraz UDP,
        ii. Wykrywanie duplikacji adresu IP,
        iii. Atak zatruwania ARP,
        iv. Nieprawidłowa długość pakietu TCP oraz UDP.
    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        i. RDP,
        ii. SMB,
        iii. MySQL,
        iv. MSSQL.
    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    A. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        i. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        iii. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
        iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   i. RedHat Enterprise Linux (RHEL),
   ii. Rocky Linux,
   iii. Ubuntu,
   iv. Debian,
   v. SUSE Linux Enterprise Server (SLES),
   vi. Oracle Linux,
   vii. Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   i. Wirus.
   ii. Trojan.
   iii. Robak.
   iv. Adware.
   v. Spyware.
   vi. Dialer.
   vii. Phishing.
   viii. Backdoor.
3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

i. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
ii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   i. całego dysku,
   ii. wybranych katalogów,
   iii. pojedynczych plików,
   iv. plików spakowanych oraz skompresowanych,
   v. dysków sieciowych,
   vi. dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   i. wybranych plików,
   ii. wybranych procesów,
   iii. wybranych lokalizacji,
   iv. wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    v. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
    i. proces budowania obrazu kontenera,
    ii. wdrażanie obrazu kontenera.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
   A. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
      i. Android,
      ii. iOS,
      iii. iPadOS.
   B. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
      i. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
      ii. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
      iii. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
      iv. Apple Business Manager (ABM),
      v. Android Enterprise (co najmniej w zakresie Device Owner).
2. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
      i. usunięcie zawartości urządzenia,
      ii. przywrócenie urządzenia do ustawień fabrycznych,
      iii. zablokowanie urządzenia,
      iv. uruchomienie sygnału dźwiękowego,
      v. lokalizację GPS,
      vi. Resetowanie hasła blokady ekranu.
3. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
4. MDM musi umożliwiać co najmniej:
   A. Dla systemów iOS oraz iPadOS
      i. konfigurację kont e-mail,
      ii. konfigurację połączeń VPN,
      iii. konfigurację połączeń Wi-Fi,

iv. konfigurację listy certyfikatów,
v. możliwość uruchomienia trybu jednej aplikacji.

B. Dla systemu Android:
i. blokadę wykonywania połączeń,
ii. blokadę konfiguracji sieci Wi-Fi,
iii. blokadę konfiguracji tuneli VPN,
iv. zarządzenie aktualizacjami sytemu operacyjnego,
v. blokadę zmiany tapety urządzenia.

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
   i. Tworzenie procesów.
   ii. Uruchamianie, zatrzymanie i modyfikacja usług.
   iii. Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym.
   iv. Usuwanie oraz zmiana nazw plików.
   v. Tworzenie i usuwanie kluczy rejestru systemowego.
   vi. Ładowanie bibliotek DLL.
   vii. Zalogowanie użytkowników.
4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
   A. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
      i. Blokowanie pliku wykonywalnego.
      ii. Blokowanie pliku wykonywalnego i poddanie go kwarantannie.
      iii. Blokowanie podejrzanej biblioteki DLL.
      iv. Zakończenie procesu.

v. Skanowanie komputera w poszukiwaniu zagrożeń.
vi. Wyłączenie komputera.
vii. Izolacja sieciowa hosta dla systemów Windows oraz Linux.
viii. Wylogowanie użytkownika.

B. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
   A. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
   B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
      i. Proces.
      ii. Proces nadrzędny (proces rodzica).
      iii. Nazwę procesu.
      iv. Ścieżkę procesu.
      v. Wiersz polecenia.
      vi. Wydawcę.
      vii. Typ podpisu cyfrowego.
      viii. SHA-1.
      ix. SHA-2.
      x. Użytkownika.
   C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
   A. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
   B. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
      i. SHA-1.
      ii. SHA-256.
7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:

i. Hash pliku SHA-1.
ii. Hash pliku SHA-256.
iii. Hash pliku MD5.
iv. Typ sygnatury podpisu cyfrowego.
v. Wydawcę certyfikatu.
vi. Wersję pliku.
vii. Oryginalną nazwę pliku.
viii. Rozmiar pliku.
ix. Reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego.
x. Pierwsze uruchomienie pliku w środowisku.
xi. Ostatnie uruchomienie pliku w środowisku.

8. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
   i. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
   ii. Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
   iii. Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
   iv. Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
   v. Administrator musi posiadać możliwość odczytania informacji o języku skryptu.
9. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
   i. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
10. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
11. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
12. Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR, przynajmniej w oparciu o:

i. Wyszukiwanie dowolnego tekstu.
ii. Wyszukiwanie, pozwalające łączyć ze sobą różne słowa, oddalone od siebie nie więcej niż 3 innymi słowami.
iii. Wyszukiwanie po nazwie procesów.
iv. Wyszukiwanie po ocenie ryzyka.
v. Filtrowanie według daty.

Oprogramowanie do monitorowania infrastruktury informatycznej

Oferowane rozwiązanie musi być dostarczone w modelu licencji bezterminowej (perpetual) lub licencji open source niewymagającej odnawiania prawa do korzystania z oprogramowania. Zamawiający musi uzyskać prawo do bezterminowego użytkowania wszystkich dostarczonych komponentów systemu monitorowania infrastruktury IT, bez ograniczeń czasowych dotyczących funkcjonalności podstawowych. Dopuszcza się rozwiązania typu open source udostępniane na podstawie licencji otwartych, zapewniających możliwość nieograniczonego czasowo użytkowania, instalacji, konfiguracji, aktualizacji oraz rozbudowy systemu bez ponoszenia kosztów licencyjnych za samo oprogramowanie. W przypadku gdy producent oferuje opcjonalne usługi wsparcia technicznego, subskrypcje, szkolenia lub usługi dodatkowe, nie mogą one być wymagane do działania podstawowych funkcji systemu po zakończeniu okresu wdrożenia. Zamawiający musi zachować możliwość dalszego korzystania z rozwiązania po zakończeniu okresu wsparcia producenta lub wykonawcy. System nie może posiadać ograniczeń licencyjnych dotyczących liczby monitorowanych urządzeń, użytkowników, elementów monitorowanych (items), alarmów, dashboardów ani czasu przechowywania danych wynikających wyłącznie z modelu licencjonowania.

W ramach wdrożenia Zamawiający oczekuje:

1. Utworzenia maszyn wirtualnych do instalacji oprogramowania,
2. Instalacji i wstępnej konfiguracji oprogramowania,
3. Parametryzacji oprogramowania zgodnie z przygotowanym projektem, co najmniej w zakresie:
    a. Monitoring zasobów serwerowych (CPU, RAM, pamięć masowa),

b. Monitoring dostępności wszystkich hostów,

c. Monitoring dostępności usług WWW,

d. Konfiguracja kokpitów,

e. Konfiguracja powiadomień.

4. Przeprowadzenie testów systemu,

5. Przeprowadzanie szkoleń stanowiskowych dla administratora.

System musi spełniać następujące wymagania:

Cecha	**Wymagania minimalne**
Ogólne	Głównym zadaniem do realizacji przez system monitoringu jest zarządzanie wydajnością i dostępnością w zakresie komponentów tj.: - serwery - urządzenia sieciowe - bazy danych - aplikacje System musi wspomagać administrowaniu w proaktywnym zarządzaniu kondycją infrastruktury IT identyfikując potencjalne problemy i awarie, zanim wpłyną one negatywnie na działanie Urzędu.
	System musi umożliwiać monitorowanie urządzeń zarówno w sposób agentowy jak i bezagentowy (sieciowy)

	System musi umożliwiać monitorowanie agentowe co najmniej systemów: - Microsoft Windows - Linux (dowolna dystrybucja) - MacOS
	System musi posiadać możliwość monitorowanie bezagentowego dostępności i wydajności dowolnej witryny WWW
	System musi umożliwiać bezagentowy monitoring z wykorzystaniem protokołów SNMP
	System musi być dostarczony na licencji umożliwiającej na monitorowanie dowolnej liczby komponentów IT i pracę dowolnej liczby operatorów
	System musi posiadać narzędzia do zbierania danych o wydajności i dostępności usług
	System musi umożliwiać konfigurację interwałów i częstotliwości monitoringu poszczególnych komponentów lub grup komponentów
	System musi posiadać narzędzia umożliwiające wizualizację danych w postaci wykresów
	System musi umożliwiać budowanie map infrastruktury sieci oraz osadzania komponentów na mapach

	System musi posiadać mechanizm alertów z możliwością ich wysyłki co najmniej przez email, sms, MS Teams
	System musi posiadać API umożliwiającego integrację z innymi narzędziami
	System musi posiadać funkcję wykrywania anomalii oraz monitorowania trendów
	System musi posiadać możliwość definiowania i zamawiania okresowych raportów dotyczących kondycji środowiska
	System musi posiadać mechanizm budowania dedykowanych kokpitów do monitoringu
	Komunikacja pomiędzy wszystkimi komponentami systemu musi odbywać się z wykorzystaniem bezpiecznych i szyfrowanych połączeń
	System musi posiadać rozbudowany moduł zarządzania użytkownikami, grupami użytkowników oraz uprawnieniami
	System musi umożliwiać uwierzytelnianie użytkowników przy pomocy: - kont wbudowanych - usługi katalogowej LDAP/AD - usługi pojedynczego logowania SSO

	System musi posiadać narzędzia do automatycznego wykrywania i podłączania komponentów

Oprogramowanie do inwentaryzacji ITSM wraz usługą inwentaryzacji aktywów teleinformatycznych

Oferowane rozwiązanie musi być dostarczone w modelu licencji bezterminowej (perpetual) lub licencji open source niewymagającej odnawiania prawa do korzystania z oprogramowania. Zamawiający musi uzyskać prawo do bezterminowego użytkowania wszystkich dostarczonych komponentów systemu monitorowania infrastruktury IT, bez ograniczeń czasowych dotyczących funkcjonalności podstawowych. Dopuszcza się rozwiązania typu open source udostępniane na podstawie licencji otwartych, zapewniających możliwość nieograniczonego czasowo użytkowania, instalacji, konfiguracji, aktualizacji oraz rozbudowy systemu bez ponoszenia kosztów licencyjnych za samo oprogramowanie. W przypadku gdy producent oferuje opcjonalne usługi wsparcia technicznego, subskrypcje, szkolenia lub usługi dodatkowe, nie mogą one być wymagane do działania podstawowych funkcji systemu po zakończeniu okresu wdrożenia. Zamawiający musi zachować możliwość dalszego korzystania z rozwiązania po zakończeniu okresu wsparcia producenta lub wykonawcy. System nie może posiadać ograniczeń licencyjnych dotyczących liczby urządzeń, użytkowników, elementów (items) ani czasu przechowywania danych wynikających wyłącznie z modelu licencjonowania.

Zamawiający oczekuje przeprowadzenie inwentaryzacji aktywów informatycznych Zamawiającego wraz z dostawą, instalacją i konfiguracją narzędzia wspierającego zarządzanie zasobami IT (zgodnego z wymaganiami zestawionymi w tabeli) umożliwiającego ewidencjonowanie sprzętu komputerowego, urządzeń sieciowych, serwerów, licencji, akcesoriów, komponentów, lokalizacji, użytkowników oraz przypisań zasobów. Wykonawca zobowiązany będzie do wdrożenia systemu w środowisku wskazanym przez Zamawiającego, skonfigurowania podstawowych słowników, kategorii, statusów, lokalizacji, ról i uprawnień, a także zaimportowania lub wprowadzenia danych pozyskanych w ramach inwentaryzacji. W ramach realizacji usługi Wykonawca powinien uporządkować informacje o aktywach, przypisać je do właściwych komórek organizacyjnych lub użytkowników, oznaczyć ich status eksploatacyjny oraz

przygotować Zamawiającego do bieżącego prowadzenia ewidencji, raportowania i kontroli cyklu życia zasobów informatycznych. Bo najwyraźniej nawet laptopy muszą mieć swoją biografię, status społeczny i miejsce zamieszkania w systemie.

Cecha	**Wymagania minimalne**
Ogólne	Platforma musi umożliwiać ewidencję zasobów informatycznych Zamawiającego oraz zarządzanie ich cyklem życia w organizacji.

	W ramach platformy musi istnieć możliwość zarządzania:
	• Zasoby IT
	  ○ Identyfikator
	  ○ Numer seryjny
	  ○ Kategoria
	  ○ Data zakupu
	  ○ Data ważności gwarancji
	  ○ Lokalizacja
	  ○ Aktualny użytkownik
	  ○ Zdjęcie
	• Licencje
	  ○ Nazwa
	  ○ Klucz produktu
	  ○ Producent
	  ○ Liczba sztuk
	  ○ Data ważności
	• Akcesoria
	• Komponenty (części)
	• Zestawy komputerowe
	• Materiały eksploatacyjne

	Platforma musi być zainstalowana w infrastrukturze Zamawiającego.

	Platforma musi udostępniać swój interfejs użytkownika za pomocą portalu www, bez konieczności instalowania jakiegokolwiek oprogramowania po stronie komputera użytkownika.
	Dostęp do platformy musi być możliwy do ograniczenia ze wskazanych adresów IP lub całych podsieci.
	Autoryzacja użytkowników w ramach platformy musi być możliwa za pomocą kont wbudowanych, usługi katalogowej LDAP oraz usługi SSO (co najmniej SAML).
	Platforma musi umożliwiać włączenia do wybranych użytkowników drugiego składnika autoryzacji (2FA), minimalnie za pomocą Google Authenticator.
	Interfejs użytkownika (GUI) platformy musi być w języku polskim.
	GUI musi umożliwiać personalizacje wyglądu platformy co namniej w zakresie zmiany kolorów, zarządzania logo, zarządzania nagłówkiem i stopką oraz modyfikacji styli CSS.
	Platforma musi posiadać wbudowany mechanizm powiadomień umożliwiający wysyłkę email np. w przypadku wygaśnięcia licencji lub gwarancji.
	Platforma musi obsługiwać mechanizm przydzielania danego zasobu użytkownikowi oraz zwrotu, dodatkowo musi istnieć mechanizm akcji masowych np. zwrot wszystkich zasobów posiadanych przez użytkownika w przypadku zakończenia umowy.
	Platforma musi umożliwiać obsługę podpisów odręcznych (np. na tablecie) przez użytkowników podczas przyjmowania na stan zasobów.
	Platforma musi umożliwiać projektowanie i drukowanie etykiet samoprzylepnych z możliwością osadzenia na nich kodu kreskowego.
	Platforma musi umożliwiać generowanie i obsługę kodów kreskowych 1D (EAN5 i EAN13) oraz 2D (QRCODE i DATAMATRIX).
	Platforma musi posiadać mechanizm tworzenia własnych pól (tekstowe, jednokrotnego wyboru, wielokrotnego wyboru), grupowania pól w sekcje oraz wprowadzania walidacji do pól z wykorzystaniem wyrażeń regularnych.
	Platforma musi umożliwiać zarządzanie słownikami: • Kategorie zasobów • Dostawcy • Producenci

	• Działy (departamenty) • Lokalizacje • Statusy zasobów
	Platforma musi posiadać wbudowany moduł raportowy z zestawem predefiniowanych raportów.

System klasy DLP

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie systemu klasy DLP, tj. Data Loss Prevention, przeznaczonego do ochrony danych przed nieuprawnionym ujawnieniem, wyniesieniem, przesłaniem, skopiowaniem, wydrukowaniem lub przetwarzaniem niezgodnym z przyjętymi politykami bezpieczeństwa. System musi zostać dostarczony w modelu licencji dla 20 końcówek obejmującej okres 12 miesięcy od dnia uruchomienia produkcyjnego.

System DLP musi umożliwiać centralne zarządzanie ochroną danych przetwarzanych na stacjach roboczych, serwerach, w poczcie elektronicznej. Rozwiązanie musi zapewniać możliwość tworzenia i egzekwowania polityk bezpieczeństwa dotyczących operacji na danych, w szczególności zapisywania, przenoszenia, drukowania, drukowania wirtualnego, wysyłania pocztą elektroniczną, przesyłania do chmury oraz przesyłania za pomocą komunikatorów. Reguły ochrony danych muszą być egzekwowane również w przypadku czasowego braku połączenia stacji roboczej z serwerem zarządzającym, a dane i logi zebrane lokalnie muszą być przechowywane do czasu ponownego nawiązania połączenia.

Rozwiązanie musi wspierać instalację agentów na systemach Windows 10 64-bit, Windows 11 64-bit, Windows Server 2019 lub nowszych oraz macOS 12 lub nowszych. Serwer administracyjny musi umożliwiać instalację na systemie Windows Server 2019 64-bit lub nowszym oraz współpracę z bazą danych MS SQL Server 2016 SP1 CU2 lub nowszą, MS SQL Server Express. Konsola administracyjna musi być dostępna z poziomu przeglądarki internetowej, umożliwiać pobranie pliku instalacyjnego agenta, zdalną instalację i dezinstalację klienta na stacjach roboczych, weryfikację wersji zainstalowanego oprogramowania klienckiego, aktualizację agenta oraz jego dezaktywację. Konsola administracyjna oraz komunikaty prezentowane użytkownikom końcowym muszą być dostępne w języku polskim.

System musi umożliwiać integrację z Active Directory, w tym synchronizację użytkowników, stacji roboczych oraz grup bezpieczeństwa na potrzeby logowania do konsoli zarządzającej i przypisywania polityk bezpieczeństwa. Administrator musi mieć możliwość tworzenia i usuwania kont administratorów, nadawania i odbierania uprawnień do poszczególnych modułów systemu, a także prowadzenia audytu operacji wykonywanych przez administratorów w konsoli DLP. System musi umożliwiać przypisanie wybranemu użytkownikowi trybu wyjątku, w ramach którego jego działania nie będą ograniczane przez określone polityki bezpieczeństwa, zgodnie z decyzją administratora i przyjętymi procedurami Zamawiającego.

System musi umożliwiać klasyfikowanie i kategoryzowanie danych wrażliwych na podstawie co najmniej: aplikacji źródłowej, lokalizacji, źródłowego adresu URL, formatu pliku oraz zawartości pliku. Wymagana jest możliwość wyszukiwania i ochrony plików zawierających dane wrażliwe według zdefiniowanych kryteriów, w tym co najmniej numerów kart kredytowych, numerów PESEL, numerów dowodów osobistych, numerów paszportów, numerów REGON, NIP, numerów IBAN, wyrażeń regularnych oraz określonych ciągów znaków. Weryfikacja zawartości plików musi odbywać się w czasie rzeczywistym. System musi umożliwiać wykrywanie danych wrażliwych również w zasobach lokalnych urządzeń końcowych oraz wykorzystywać mechanizm OCR do wykrywania poufnych treści w obrazach, zdjęciach i zeskanowanych dokumentach.

System musi umożliwiać tworzenie własnych kategorii dla stron internetowych, aplikacji i typów plików, filtrowanie, sortowanie i grupowanie zebranych danych w konsoli administracyjnej, a także tworzenie paneli kontrolnych dla wskazanych użytkowników, stacji roboczych lub grup w określonym przedziale czasu. Rozwiązanie musi zbierać informacje o aktywności użytkowników i urządzeń, w tym co najmniej o uruchomionych aplikacjach, podłączonych urządzeniach, odwiedzanych stronach internetowych, wydrukowanych dokumentach, wysyłanych i odbieranych wiadomościach e-mail oraz czynnościach wykonywanych na plikach. System musi również zbierać informacje o podłączanych urządzeniach, odwiedzanych domenach internetowych, ścieżkach sieciowych oraz drukarkach lokalnych i sieciowych, z możliwością dodawania tych lokalizacji do kategorii bezpiecznych lub niezaufanych bez konieczności ręcznego wpisywania ścieżek lub numerów seryjnych.

Rozwiązanie musi umożliwiać tworzenie polityk dostępu do lokalizacji i kanałów transferu danych, w tym przypisywanie indywidualnych zasad dla lokalizacji bezpiecznych, niezaufanych lub nieprzypisanych. System musi pozwalać na określenie akcji podejmowanych w przypadku naruszenia polityki, takich jak zapisanie logu, powiadomienie użytkownika, blokowanie operacji lub blokowanie operacji z możliwością zastąpienia decyzji przez użytkownika, o ile taka funkcjonalność zostanie dopuszczona przez Zamawiającego. System powinien wspierać polityki dynamiczne, w których akcja może być zależna od profilu pracy użytkownika oraz wyniku działania mechanizmów analitycznych lub uczenia maszynowego. Polityki dynamiczne powinny mieć możliwość działania co najmniej w trybie standardowym i łagodnym, z możliwością przypisania ich do wybranych użytkowników.

System musi zapewniać mechanizmy powiadamiania użytkownika końcowego o naruszeniu reguł DLP, z możliwością dostosowania treści i wyglądu komunikatu, w tym grafiki, adresu e-mail oraz odnośnika do polityki bezpieczeństwa Zamawiającego. System musi umożliwiać wysyłanie alertów co najmniej za pośrednictwem wiadomości e-mail oraz protokołu SYSLOG, a także eksport logów do systemu SIEM. Konsola musi umożliwiać konfigurację lub zmianę domyślnego serwera SMTP, a serwer administracyjny powinien umożliwiać połączenie z serwerem SMTP udostępnianym przez producenta lub wskazanym przez Zamawiającego.

System musi umożliwiać tworzenie raportów na podstawie zebranych logów, z możliwością dostosowania filtrów, użytkowników, zakresu czasu oraz układu prezentowanych danych. Wymagana jest możliwość generowania raportu zawierającego podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami, w tym w formie cyklicznej. System musi posiadać mechanizm zarządzania retencją danych, w szczególności usuwania najstarszych informacji po osiągnięciu domyślnego lub skonfigurowanego limitu rozmiaru bazy danych. Wymagana jest również możliwość podłączenia archiwum logów w formacie plików o rozszerzeniu MDF.

W ramach usługi wdrożenia Wykonawca zobowiązany jest do przeprowadzenia instalacji i konfiguracji systemu DLP w środowisku Zamawiającego, zgodnie z wymaganiami technicznymi producenta oraz wytycznymi Zamawiającego. Wdrożenie musi obejmować co najmniej przygotowanie środowiska serwerowego, instalację serwera administracyjnego, konfigurację bazy danych, konfigurację konsoli administracyjnej, integrację z Active Directory, przygotowanie ról i uprawnień administratorów,

konfigurację podstawowych polityk bezpieczeństwa, konfigurację alertów, powiadomień, raportów, integracji z pocztą elektroniczną, SYSLOG oraz SIEM, a także przygotowanie paczki instalacyjnej agenta i wdrożenie agentów na wskazanej liczbie stacji roboczych lub serwerów objętych zamówieniem.

Wykonawca zobowiązany jest do przeprowadzenia konfiguracji początkowej polityk DLP w uzgodnieniu z Zamawiającym, z uwzględnieniem charakteru przetwarzanych danych, struktury organizacyjnej, grup użytkowników, lokalizacji, kanałów komunikacji oraz ryzyk związanych z możliwością nieuprawnionego wyniesienia danych. W szczególności Wykonawca powinien przygotować polityki obejmujące ochronę danych osobowych, identyfikatorów krajowych, danych finansowych, dokumentów wewnętrznych, danych przesyłanych pocztą elektroniczną, danych kopiowanych na nośniki zewnętrzne, danych drukowanych oraz danych przesyłanych do usług chmurowych i komunikatorów. Zakres blokowania, ostrzegania, logowania i raportowania musi zostać uzgodniony z Zamawiającym, tak aby wdrożenie nie powodowało nieuzasadnionego zakłócenia pracy użytkowników.

Wykonawca zobowiązany jest do przeprowadzenia testów poprawności działania systemu po wdrożeniu, obejmujących co najmniej weryfikację działania agentów, komunikacji z serwerem administracyjnym, synchronizacji z Active Directory, egzekwowania polityk DLP, generowania alertów, wysyłki powiadomień, eksportu logów do SIEM/SYSLOG, raportowania oraz działania mechanizmów ochrony danych w poczcie elektronicznej. Wyniki testów muszą zostać udokumentowane w protokole lub raporcie powdrożeniowym.

W ramach realizacji zamówienia Wykonawca zobowiązany jest do przekazania Zamawiającemu dokumentacji powdrożeniowej obejmującej co najmniej opis architektury wdrożonego rozwiązania, opis konfiguracji serwera administracyjnego, bazy danych, integracji, ról i uprawnień, polityk bezpieczeństwa, alertów, raportów oraz zasad eksploatacji systemu. Dokumentacja musi zawierać również podstawowe instrukcje administracyjne dotyczące zarządzania agentami, użytkownikami, politykami, raportami, alertami oraz sposobem postępowania w przypadku wykrycia naruszenia polityk DLP.

Wykonawca zobowiązany jest do przeprowadzenia instruktażu lub szkolenia administratorów wskazanych przez Zamawiającego z zakresu obsługi systemu DLP, w szczególności zarządzania konsolą administracyjną, tworzenia i modyfikacji polityk, analizy incydentów, przeglądu logów, generowania raportów, obsługi alertów, zarządzania agentami oraz podstawowej diagnostyki problemów. Szkolenie powinno obejmować część praktyczną opartą na konfiguracji wdrożonej u Zamawiającego

W okresie obowiązywania licencji Wykonawca zapewni Zamawiającemu prawo do korzystania z systemu, aktualizacji oraz wsparcia producenta lub równoważnego wsparcia technicznego, zgodnie z warunkami licencji oferowanego rozwiązania. Wykonawca zobowiązany jest do dostarczenia licencji, kluczy, danych dostępowych lub innych informacji niezbędnych do legalnego korzystania z systemu przez okres 12 miesięcy, a także do potwierdzenia zakresu licencji w dokumentacji odbiorowej.

Usługa segmentacji sieci

Zamawiający wymaga opracowanie i wdrożenia projektu segmentacji sieci zgodnie z najwyższymi standardami branżowymi dotyczącymi bezpieczeństwa. Usługa zostanie wykonana zarówno w ramach posiadanego sprzętu (tam gdzie jest to możliwe) oraz z wykorzystaniem sprzętu i oprogramowania dostarczanego w ramach realizacji przedmiotu zamówienia.

Usługa konfiguracji i hardeningu systemów operacyjnych oraz urządzeń sieciowych (audyt cyberbezpieczeństwa sieci)

Przedmiotem usługi jest przeprowadzenie konfiguracji oraz hardeningu systemów operacyjnych i urządzeń sieciowych Zamawiającego w celu zwiększenia poziomu bezpieczeństwa środowiska teleinformatycznego oraz ograniczenia ryzyka wykorzystania znanych podatności. Usługa obejmuje analizę obecnej konfiguracji, identyfikację podatności i słabości bezpieczeństwa, priorytetyzację działań z uwzględnieniem klasyfikacji CVE oraz oceny ryzyka według CVSS, a następnie wdrożenie uzgodnionych zmian konfiguracyjnych.
W ramach realizacji usługi Wykonawca zobowiązany będzie do weryfikacji i wzmocnienia konfiguracji systemów operacyjnych, serwerów, usług systemowych oraz urządzeń sieciowych, w szczególności w zakresie kont użytkowników, uprawnień administracyjnych, polityk haseł, dostępu zdalnego, usług

sieciowych, protokołów administracyjnych, aktualizacji bezpieczeństwa, logowania zdarzeń, synchronizacji czasu, lokalnych zapór systemowych oraz kopii konfiguracji.

Wykonawca zobowiązany jest realizować prace z zachowaniem ciągłości działania środowiska Zamawiającego. Przed wdrożeniem zmian Wykonawca wykona kopię konfiguracji oraz uzgodni z Zamawiającym zakres działań mogących mieć wpływ na dostępność usług. Wszystkie działania muszą być prowadzone w sposób bezpieczny, kontrolowany i zgodny z dobrymi praktykami cyberbezpieczeństwa.

Hardening systemów operacyjnych (serwery i stacje robocze) powinien obejmować w szczególności zakres zestawiony w tabeli.

Zakres	**Wymaganie**
Konta użytkowników	Przegląd kont lokalnych i administracyjnych, wyłączenie lub ograniczenie kont nieużywanych, domyślnych lub nadmiarowych
Hasła i uwierzytelnianie	Wdrożenie lub weryfikacja polityk haseł, blokady kont, zasad zmiany haseł oraz, jeżeli możliwe, uwierzytelniania wieloskładnikowego
Uprawnienia	Ograniczenie uprawnień użytkowników i usług do minimalnego wymaganego poziomu
Usługi systemowe	Wyłączenie zbędnych usług, demonów, portów i komponentów systemowych
Dostęp zdalny	Ograniczenie dostępu zdalnego do systemów i urządzeń, w tym stosowanie bezpiecznych protokołów oraz ograniczeń adresowych
Protokoły administracyjne	Wyłączenie protokołów nieszyfrowanych lub podatnych na przechwycenie danych, takich jak Telnet, FTP, HTTP dla paneli administracyjnych, jeżeli nie są niezbędne
SNMP	Weryfikacja konfiguracji SNMP, w szczególności ograniczenie dostępu, zmiana domyślnych community string oraz preferowanie bezpieczniejszych wersji protokołu
Aktualizacje	Weryfikacja poziomu aktualności systemów, firmware, sterowników, bibliotek i komponentów zależnych
Firewall lokalny	Konfiguracja lub weryfikacja lokalnych reguł zapory systemowej

Rejestrowanie zdarzeń	Włączenie i ujednolicenie logowania zdarzeń istotnych z punktu widzenia bezpieczeństwa
Synchronizacja czasu	Weryfikacja konfiguracji synchronizacji czasu, niezbędnej dla poprawnej korelacji zdarzeń bezpieczeństwa
Kopie zapasowe konfiguracji	Wykonanie kopii konfiguracji urządzeń i systemów przed oraz po zmianach
Zgodność z CVE/CVSS	Przypisanie wykrytych podatności do znanych identyfikatorów CVE, jeżeli dotyczy, oraz określenie priorytetu działań według poziomu ryzyka CVSS

Hardening urządzeń sieciowych powinien obejmować w szczególności zakres zestawiony w tabeli.

Zakres	Wymaganie
Inwentaryzacja urządzeń sieciowych	Identyfikacja urządzeń objętych usługą, w tym punktów dostępowych Wi-Fi, przełączników, routerów, kontrolerów WLAN, urządzeń brzegowych oraz innych elementów infrastruktury sieciowej.
Weryfikacja wersji oprogramowania	Sprawdzenie wersji firmware/oprogramowania urządzeń oraz ocena dostępności aktualizacji bezpieczeństwa eliminujących znane podatności.
Analiza podatności CVE/CVSS	Weryfikacja znanych podatności dla wykorzystywanego firmware, systemu zarządzania i usług urządzenia, z priorytetyzacją podatności krytycznych i wysokich według klasyfikacji CVSS.
Aktualizacja firmware	Rekomendacja lub wykonanie aktualizacji firmware urządzeń sieciowych, o ile jest to możliwe i uzgodnione z Zamawiającym, z uwzględnieniem ryzyka wpływu na dostępność usług.
Kopia konfiguracji	Wykonanie kopii konfiguracji urządzeń przed rozpoczęciem prac oraz po zakończeniu hardeningu.
Kontrola kont administracyjnych	Przegląd kont administracyjnych, usunięcie lub wyłączenie kont nieużywanych, domyślnych i nadmiarowych oraz ograniczenie dostępu do kont uprzywilejowanych.
Polityka haseł	Weryfikacja i wdrożenie silnych haseł administracyjnych, zgodnych z polityką bezpieczeństwa Zamawiającego.

Uwierzytelnianie administratorów	Weryfikacja możliwości zastosowania centralnego uwierzytelniania administratorów, np. LDAP, RADIUS, TACACS+ lub rozwiązania równoważnego.
MFA dla panelu administracyjnego	Weryfikacja możliwości włączenia uwierzytelniania wieloskładnikowego dla dostępu administracyjnego, jeżeli urządzenie lub system zarządzania wspiera taką funkcję.
Ograniczenie dostępu administracyjnego	Ograniczenie dostępu do paneli administracyjnych urządzeń wyłącznie z określonych adresów IP, VLAN-ów administracyjnych lub stacji zarządzających.
Bezpieczne protokoły zarządzania	Wyłączenie nieszyfrowanych protokołów zarządzania, takich jak Telnet, HTTP, FTP, TFTP, jeżeli nie są niezbędne, oraz preferowanie SSH, HTTPS, SFTP/SCP lub rozwiązań równoważnych.
Zmiana domyślnych portów/usług	Weryfikacja możliwości ograniczenia lub zmiany domyślnie dostępnych usług administracyjnych, jeżeli jest to uzasadnione i nie wpływa negatywnie na utrzymanie środowiska.
Wyłączenie nieużywanych usług	Wyłączenie zbędnych usług sieciowych i administracyjnych, w tym usług diagnostycznych, discovery, UPnP, WPS, Bonjour/mDNS lub innych funkcji niewykorzystywanych przez Zamawiającego.
Segmentacja sieci zarządzającej	Weryfikacja lub wdrożenie separacji ruchu administracyjnego od ruchu użytkowników, w tym wykorzystanie dedykowanego VLAN-u zarządzającego.
Konfiguracja VLAN	Weryfikacja poprawności przypisania SSID, portów uplink, trunk/access oraz separacji sieci produkcyjnych, gościnnych, administracyjnych i technicznych.
Separacja sieci Wi-Fi	Weryfikacja rozdzielenia sieci Wi-Fi dla pracowników, gości, urządzeń technicznych/IoT oraz ewentualnych sieci serwisowych.
Bezpieczeństwo SSID	Przegląd konfiguracji SSID, ukrycie lub usunięcie nieużywanych SSID, weryfikacja nazewnictwa oraz ograniczenie ujawniania informacji o organizacji lub przeznaczeniu sieci.

Szyfrowanie Wi-Fi	Weryfikacja zastosowanego standardu szyfrowania i rekomendacja stosowania WPA2-Enterprise, WPA3-Enterprise lub równoważnych mechanizmów, jeżeli są wspierane przez środowisko.
Eliminacja słabych standardów	Wyłączenie przestarzałych lub podatnych mechanizmów zabezpieczeń, w szczególności WEP, WPA/WPA1, TKIP oraz otwartych sieci produkcyjnych.
WPS	Wyłączenie funkcji WPS na punktach dostępowych, jeżeli jest dostępna, z uwagi na ryzyko nieautoryzowanego dostępu.
Uwierzytelnianie użytkowników Wi-Fi	Weryfikacja możliwości integracji sieci Wi-Fi z usługą katalogową, serwerem RADIUS lub innym centralnym mechanizmem uwierzytelniania.
Sieć gościnna	Weryfikacja konfiguracji sieci gościnnej, w tym izolacji od sieci wewnętrznej, ograniczenia czasu sesji, akceptacji regulaminu, captive portal lub innych mechanizmów kontroli dostępu.
Izolacja klientów Wi-Fi	Włączenie izolacji klientów w sieciach, w których komunikacja pomiędzy urządzeniami końcowymi nie jest wymagana, w szczególności w sieci gościnnej.
Ograniczenie dostępu do zasobów wewnętrznych	Weryfikacja reguł dostępu z sieci Wi-Fi do zasobów LAN, systemów administracyjnych, serwerów, urządzeń OT/ICS oraz usług krytycznych.
Kontrola adresacji DHCP	Weryfikacja zakresów DHCP, rezerwacji adresów, bram, DNS oraz separacji adresacji pomiędzy poszczególnymi sieciami Wi-Fi i VLAN.
Filtrowanie ruchu	Weryfikacja reguł firewall/ACL dla ruchu generowanego przez klientów Wi-Fi oraz urządzenia zarządzające.
Ograniczenie komunikacji między VLAN	Weryfikacja zasad routingu i dostępu pomiędzy VLAN-ami, w szczególności pomiędzy siecią gościnną, produkcyjną, administracyjną i techniczną.
Dostęp do infrastruktury OT/ICS	Weryfikacja, czy sieci Wi-Fi nie zapewniają nieuzasadnionego dostępu do środowisk technologicznych, przemysłowych lub systemów sterowania.

SNMP	Weryfikacja konfiguracji SNMP, wyłączenie wersji nieużywanych, zmiana domyślnych community string, ograniczenie dostępu adresowego oraz preferowanie SNMPv3, jeżeli jest wspierane.
Logowanie zdarzeń	Włączenie lub weryfikacja logowania zdarzeń administracyjnych, zmian konfiguracji, prób logowania, rozłączeń, restartów urządzeń oraz błędów pracy.
Integracja z systemem logowania/SIEM	Konfiguracja lub weryfikacja wysyłania logów do centralnego systemu logowania lub systemu klasy SIEM, jeżeli taki system jest wdrażany lub eksploatowany przez Zamawiającego.
Integracja z monitoringiem	Weryfikacja możliwości monitorowania dostępności, obciążenia, liczby klientów, jakości sygnału, wykorzystania pasma i stanu urządzeń w systemie monitorowania infrastruktury.
Synchronizacja czasu	Weryfikacja konfiguracji NTP/SNTP w celu zapewnienia spójnych znaczników czasu w logach i zdarzeniach bezpieczeństwa.
Alertowanie	Weryfikacja lub konfiguracja alertów dotyczących awarii AP, przeciążenia, nieautoryzowanych prób logowania, zmian konfiguracji, utraty łączności lub wykrycia nietypowego zachowania.
Rogue AP	Weryfikacja możliwości wykrywania nieautoryzowanych punktów dostępowych lub sieci podszywających się pod sieć Zamawiającego, jeżeli urządzenia wspierają taką funkcję.
Moc nadawcza i kanały	Weryfikacja ustawień mocy nadawczej, kanałów radiowych oraz planu radiowego w celu ograniczenia zakłóceń i nieuzasadnionego promieniowania sygnału poza obszar Zamawiającego.
Dostęp fizyczny do AP	Weryfikacja podstawowych zabezpieczeń fizycznych punktów dostępowych, w tym lokalizacji, możliwości nieautoryzowanego odłączenia lub resetu urządzenia.
Blokada resetu/funkcji lokalnych	Weryfikacja możliwości ograniczenia resetu urządzenia do ustawień fabrycznych lub nieautoryzowanej lokalnej zmiany konfiguracji, jeżeli urządzenie wspiera takie mechanizmy.

Porty uplink AP	Weryfikacja konfiguracji portów przełączników, do których podłączone są AP, w tym VLAN, trunking, native VLAN, zabezpieczenia portu oraz ograniczenie nieuprawnionego dostępu.
Zabezpieczenia portów switchy	Weryfikacja możliwości zastosowania port security, BPDU Guard, DHCP Snooping, Dynamic ARP Inspection, 802.1X lub równoważnych mechanizmów ochronnych, jeżeli są wspierane.
Administracja kontrolerem WLAN	Weryfikacja zabezpieczenia systemu centralnego zarządzania punktami dostępowymi, w tym kont, uprawnień, protokołów, logowania i kopii konfiguracji.
Profile konfiguracyjne AP	Uporządkowanie profili konfiguracyjnych, grup AP, polityk radiowych, polityk bezpieczeństwa i mapowania SSID do VLAN.
Wyłączenie starych standardów radiowych	Weryfikacja zasadności wyłączenia przestarzałych standardów transmisji, które mogą obniżać bezpieczeństwo lub wydajność sieci.
Ograniczenie pasma	Weryfikacja lub konfiguracja limitów pasma dla sieci gościnnych, testowych lub urządzeń o niskim priorytecie.
Dokumentacja konfiguracji	Opracowanie dokumentacji opisującej zastosowane ustawienia bezpieczeństwa, podział sieci, SSID, VLAN, reguły dostępu i konfigurację administracyjną.
Testy po zmianach	Przeprowadzenie testów poprawności działania sieci Wi-Fi i urządzeń sieciowych po wdrożeniu zmian, w tym testów logowania, dostępu do zasobów i działania usług.
Rekomendacje dalszych działań	Przekazanie rekomendacji dotyczących dalszego utrzymania bezpieczeństwa urządzeń sieciowych, aktualizacji, monitorowania oraz cyklicznego przeglądu konfiguracji.

Po zakończeniu prac Wykonawca (na żądanie Zamawiającego) przekaże dokumentację powykonawczą zawierającą opis wykonanych czynności, wykaz wdrożonych zmian, zidentyfikowane podatności i słabości konfiguracyjne, odniesienie do klasyfikacji CVE/CVSS tam, gdzie ma to zastosowanie, wyniki testów poprawności działania oraz rekomendacje dotyczące dalszego utrzymania bezpieczeństwa systemów i urządzeń.

Dostawa certyfikatów SSL typu wildcard

Zamawiający wymaga dostawy certyfikatu SSL klasy Thawte Wilcard SSL lub równoważnego na okres 1 roku.

Usługa klasy SASE VPN

Przedmiotem zamówienia jest dostarczenie, uruchomienie oraz konfiguracja usługi klasy SASE (Secure Access Service Edge) lub ZTNA (Zero Trust Network Access), świadczonej w modelu chmurowym, przeznaczonej do zapewnienia bezpiecznego zdalnego dostępu do zasobów teleinformatycznych Zamawiającego. Usługa ma zostać dostarczona na okres 12 miesięcy i obejmować licencje dla minimum 20 użytkowników.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do wykonania wdrożenia obejmującego w szczególności:

- dostarczenie i aktywację usługi na okres 12 miesięcy,
- konfigurację środowiska po stronie usługi,
- konfigurację połączenia pomiędzy usługą a siecią Zamawiającego z wykorzystaniem dedykowanego konektora, tunelu lub rozwiązania równoważnego,
- konfigurację polityk dostępu zgodnie z wymaganiami Zamawiającego,
- instalację i konfigurację oprogramowania klienckiego na maksymalnie 20 stacjach roboczych użytkowników,
- przeprowadzenie testów poprawności działania wdrożonego rozwiązania,
- przekazanie dokumentacji powdrożeniowej obejmującej opis konfiguracji oraz instrukcję podstawowej administracji rozwiązaniem.

Usługa musi spełniać zestawione w tabeli wymagania minimalne:

Parametr	Wymaganie minimalne
Typ rozwiązania	Usługa klasy SASE (Secure Access Service Edge) lub ZTNA (Zero Trust Network Access) umożliwiająca bezpieczny zdalny dostęp do zasobów organizacji bez konieczności zestawiania klasycznych tuneli VPN.

Liczba użytkowników	Licencja dla minimum 20 użytkowników.
Dostęp do zasobów	Możliwość bezpiecznego dostępu do zasobów znajdujących się w sieci lokalnej Zamawiającego bez konieczności publikowania usług do Internetu.
Tunel do sieci	Możliwość zestawienia szyfrowanego tunelu pomiędzy infrastrukturą Zamawiającego a usługą chmurową z wykorzystaniem dedykowanego konektora lub agenta.
Uwierzytelnianie	Obsługa lokalnych kont użytkowników oraz integracji z zewnętrznymi dostawcami tożsamości (LDAP, Active Directory, Microsoft Entra ID, Google Workspace lub równoważne).
Wieloskładnikowe uwierzytelnianie (MFA)	Obsługa uwierzytelniania wieloskładnikowego (MFA).
Autoryzacja dostępu	Możliwość definiowania polityk dostępu w oparciu o użytkownika, grupę użytkowników, adres IP, lokalizację lub urządzenie końcowe.
Aplikacja kliencka	Dostępna aplikacja kliencka dla systemów Windows oraz macOS.
Szyfrowanie	Komunikacja szyfrowana z wykorzystaniem protokołu TLS 1.2 lub nowszego.
Zarządzanie	Centralny panel administracyjny dostępny przez przeglądarkę internetową.
Rejestrowanie zdarzeń	Rejestrowanie zdarzeń logowania oraz dostępu użytkowników do zasobów.
Wysoka dostępność	Usługa świadczona z wykorzystaniem infrastruktury wysokiej dostępności po stronie dostawcy.
Aktualizacje	Aktualizacje oprogramowania realizowane przez dostawcę usługi bez konieczności ingerencji Zamawiającego.
Wdrożenie	W ramach zamówienia Wykonawca przeprowadzi konfigurację usługi, uruchomienie dostępu dla minimum 20 użytkowników, konfigurację co najmniej

	jednego tunelu do sieci Zamawiającego oraz konfigurację dostępu do minimum jednej sieci lokalnej lub jednej aplikacji wewnętrznej.
Gwarancja/ wsparcie	Świadczenie usługi oraz wsparcia technicznego przez okres minimum 12 miesięcy.

Świadczenie usługi SOC – usługa MIDS

Przedmiotem zamówienia jest świadczenie usługi monitorowania bezpieczeństwa teleinformatycznego w modelu SOC L1 i L2, realizowanej przez Wykonawcę z wykorzystaniem własnego centrum monitorowania bezpieczeństwa zlokalizowanego w serwerowni Wykonawcy przez okres do 31.12.2026 r.Usługa będzie świadczona w oparciu o dane bezpieczeństwa pochodzące z systemu klasy SIEM wdrożonego w środowisku Zamawiającego w ramach realizacji niniejszego zamówienia. System SIEM Zamawiającego będzie odpowiedzialny za zbieranie, wstępną normalizację, agregację i filtrowanie logów oraz zdarzeń bezpieczeństwa z wybranych źródeł infrastruktury IT Zamawiającego, a następnie przekazywanie uzgodnionego zakresu danych do środowiska SOC Wykonawcy.

Celem usługi jest zapewnienie bieżącego nadzoru pierwszej linii nad zdarzeniami bezpieczeństwa, identyfikacja anomalii, wykrywanie potencjalnych incydentów, wstępna kwalifikacja alertów oraz przekazywanie Zamawiającemu informacji o zdarzeniach wymagających reakcji. Usługa ma wspierać Zamawiającego w codziennym monitorowaniu stanu bezpieczeństwa infrastruktury, ograniczaniu ryzyka niezauważenia istotnych zdarzeń oraz uporządkowaniu procesu raportowania i eskalacji zdarzeń bezpieczeństwa.

Usługa SOC będzie świadczona w trybie 24/7. Usługa obejmuje podstawową analizę alertów, wstępną klasyfikację zdarzeń, identyfikację anomalii, ocenę istotności zdarzenia na podstawie dostępnych danych oraz przygotowanie informacji dla Zamawiającego.

W ramach usługi Wykonawca będzie codziennie analizował zagregowane i odfiltrowane logi oraz zdarzenia bezpieczeństwa przekazane z systemu SIEM Zamawiającego do środowiska SOC Wykonawcy. Analiza obejmie w szczególności zdarzenia wskazujące na nietypową aktywność użytkowników, próby nieuprawnionego dostępu, błędne logowania, podejrzane działania administracyjne, potencjalne naruszenia polityk bezpieczeństwa, alerty dotyczące znanych podatności, nieprawidłowości w pracy systemów oraz inne zdarzenia uznane za istotne z punktu widzenia bezpieczeństwa Zamawiającego.

Zakres usługi został zestawiony w tabeli.

Obszar	Wymaganie
Model usługi	Wykonawca zapewni świadczenie usługi SOC trybie 24/7.
Miejsce świadczenia usługi	Usługa będzie realizowana z wykorzystaniem infrastruktury SOC Wykonawcy zlokalizowanej w serwerowni Wykonawcy.

Źródło danych	Podstawowym źródłem danych dla usługi będzie system klasy SIEM wdrożony w środowisku Zamawiającego. Monitoring dotyczy zarówno sieci IT jak i OT.
Przekazywanie danych	Do środowiska SOC Wykonawcy będą przekazywane zagregowane, odfiltrowane i uzgodnione z Zamawiającym logi oraz zdarzenia bezpieczeństwa pochodzące z systemu SIEM Zamawiającego.
Zakres logów	Zakres logów przekazywanych do SOC zostanie uzgodniony na etapie wdrożenia i powinien obejmować zdarzenia istotne dla monitorowania bezpieczeństwa, w szczególności z systemów, serwerów, usług katalogowych, urządzeń sieciowych, systemów ochrony, stacji roboczych oraz innych źródeł wskazanych przez Zamawiającego.
Agregacja i filtrowanie	System SIEM Zamawiającego powinien dokonywać wstępnej agregacji i filtrowania zdarzeń, tak aby do SOC Wykonawcy trafiały dane istotne z punktu widzenia analizy bezpieczeństwa, ograniczające szum informacyjny i liczbę zdarzeń nieistotnych.
Analiza L1	Wykonawca będzie prowadził analizę pierwszej linii obejmującą wstępną ocenę alertów, klasyfikację zdarzeń, identyfikację anomalii oraz wskazanie zdarzeń wymagających reakcji Zamawiającego.
Analiza L2	Wykonawca będzie prowadził analizę drugiej linii obejmującą pogłębioną weryfikację alertów i zdarzeń zakwalifikowanych na poziomie L1 jako wymagające dalszej analizy, korelację informacji z różnych źródeł, ocenę potencjalnego wpływu na środowisko Zamawiającego, identyfikację możliwych wektorów ataku oraz przygotowanie rekomendacji działań naprawczych, ograniczających lub eskalacyjnych. Analiza L2 powinna obejmować również weryfikację fałszywie pozytywnych zgłoszeń, doprecyzowanie klasyfikacji incydentu oraz wskazanie priorytetu reakcji po stronie Zamawiającego.
Monitorowanie anomalii	Wykonawca będzie identyfikował anomalie w zdarzeniach bezpieczeństwa, w szczególności nietypowe logowania, dużą liczbę błędnych prób uwierzytelnienia, aktywność poza standardowymi godzinami, nietypowe działania administracyjne lub podejrzaną komunikację sieciową.

Wykrywanie potencjalnych incydentów	Wykonawca będzie informował Zamawiającego o zdarzeniach mogących wskazywać na incydent bezpieczeństwa, w tym próbach nieuprawnionego dostępu, naruszeniach polityk bezpieczeństwa, podejrzanej aktywności użytkowników lub systemów oraz działaniach mogących świadczyć o kompromitacji zasobu.
Informowanie o podatnościach	Wykonawca będzie informował Zamawiającego o konieczności aktualizacji lub podjęcia działań naprawczych w przypadku wykrycia zdarzeń lub alertów wskazujących na znane podatności, nieaktualne komponenty, podatne wersje oprogramowania lub konfiguracje zwiększające ryzyko naruszenia bezpieczeństwa.
Klasyfikacja zdarzeń	Wykonawca będzie klasyfikował zdarzenia według poziomu istotności, np. informacyjne, niskie, średnie, wysokie, krytyczne, zgodnie z uzgodnioną z Zamawiającym metodyką.
Eskalacja	Wykonawca będzie przekazywał Zamawiającemu informacje o zdarzeniach wymagających reakcji, wraz z podstawowym opisem, oceną istotności i rekomendowanym dalszym działaniem.
Raport dzienny	Wykonawca będzie przygotowywał codzienny raport z monitorowania bezpieczeństwa obejmujący podsumowanie analizowanych zdarzeń, wykryte anomalie, potencjalne incydenty, istotne alerty oraz rekomendacje działań po stronie Zamawiającego.
Rekomendacje	Wykonawca będzie przekazywał podstawowe rekomendacje dotyczące dalszych działań, w szczególności konieczności weryfikacji zdarzenia, aktualizacji systemu, zmiany konfiguracji, ograniczenia dostępu, sprawdzenia konta użytkownika lub podjęcia działań administracyjnych.
Dokumentowanie zdarzeń	Wykonawca będzie dokumentował zdarzenia zakwalifikowane jako istotne, w tym datę i czas wystąpienia, źródło zdarzenia, opis, poziom istotności, podjętą kwalifikację oraz przekazaną rekomendację.
Komunikacja z Zamawiającym	Wykonawca zapewni uzgodniony kanał komunikacji z Zamawiającym na potrzeby przekazywania raportów, alertów, informacji o anomaliach i potencjalnych incydentach.
Zakres odpowiedzialności	Usługa obejmuje monitoring, analizę pierwszej i drugiej linii, kwalifikację i raportowanie zdarzeń. Usługa nie obejmuje bezpośredniego usuwania skutków incydentu, prowadzenia zaawansowanej analizy malware, informatyki śledczej ani

	działań naprawczych w infrastrukturze Zamawiającego, chyba że zostanie to odrębnie określone w umowie.

Do prawidłowego działania usługi, obowiązkiem Wykonawcy jest dostarczenie, instalacja i konfiguracja w infrastrukturze Zamawiającego systemu SIEM, który stanowił będzie źródło danych dla usług SOC.

Zakres wdrożenie SIEM

Wdrożenie oprogramowania SIEM zgodnie z założeniami projektowymi, co najmniej w zakresie:

1. Instalacja oprogramowania SIEM.
2. Integracja z systemem centralnego zarządzania tożsamością.
3. Integracja z oprogramowaniem do zarządzania incydentami.
4. Przygotowanie instrukcji instalacji agentów system SIEM oraz wsparcie przy instalacji pierwszego agenta dla każdego typu wspieranego systemu operacyjnego.
5. Przygotowanie obsługi do 5 niestandardowych źródeł logów (dekodery i reguły).
6. Określenie technik i taktyk ataku zgodnie z MITRE ATT&CK dla wszystkich niestandardowych reguł, które będą tego wymagały.
7. Określenie priorytetów alarmów w celu ograniczenia „szumu informacyjnego” i eskalacji istotnych alertów.
8. Konfiguracja mechanizmów agenta SIEM do czasowego blokowania źródłowych adresów IP wykonujących brute force.
9. Konfiguracja do 2 kokpitów.
10. Konfiguracja powiadomień mailowych.

Oferowane rozwiązanie stanowiące system SIEM musi być dostarczone w modelu licencji bezterminowej (perpetual) lub licencji open source niewymagającej odnawiania prawa do korzystania z oprogramowania. Zamawiający musi uzyskać prawo do bezterminowego użytkowania wszystkich dostarczonych komponentów systemu, bez ograniczeń czasowych dotyczących funkcjonalności podstawowych. Dopuszcza się rozwiązania typu open source udostępniane na podstawie licencji otwartych, zapewniających możliwość nieograniczonego czasowo użytkowania, instalacji, konfiguracji, aktualizacji oraz rozbudowy systemu bez ponoszenia kosztów licencyjnych za samo oprogramowanie. W przypadku gdy producent oferuje opcjonalne usługi wsparcia technicznego, subskrypcje lub usługi chmurowe, nie mogą one być wymagane do działania podstawowych funkcji systemu po zakończeniu okresu wdrożenia. Zamawiający musi zachować możliwość dalszego korzystania z rozwiązania po zakończeniu okresu wsparcia producenta lub Wykonawcy.

System SIEM musi spełniać zestawione niżej wymagania funkcjonalne i techniczne.

Cecha	Wymagania minimalne
Serwer	System musi być rozwiązaniem klasy SIEM z rozszerzeniem XDR umożliwiającym monitorowanie bezpieczeństwa, wykrywania zagrożeń, monitorowania integralności oraz odpowiedzi na incydenty.
	System musi umożliwiać monitorowanie infrastruktury IT w czasie rzeczywistym. Infrastruktura IT Zamawiającego składa się z: • 6 serwerów • 2 urządzenia UTM • 3 przełączniki sieciowe • 20 komputerów użytkowników
	Komponenty serwerowe systemu muszą być możliwe do zainstalowania na systemie operacyjnym z rodziny Linux.
	System musi być możliwy do zainstalowania w środowisku wirtualizacyjnym opartym o Proxmox VE.
	Instalacja i konfiguracja systemu musi być możliwa do automatyzacji z wykorzystaniem Ansible.
	Wykonawca w ramach zamówienia dostarczy wszelkie niezbędne licencje umożliwiające uruchomienie Systemu takie jak np. systemy operacyjne, serwery baz danych, itp.
	System musi być dostarczony w konfiguracji wysokodostępnej (klaster High Availability) dla każdego z komponentów z wyłączeniem agentów.
	System musi umożliwiać monitorowanie agentowe oraz bezagentowe (sieciowe).
	Silnik system musi udostępniać API w technologii REST pozwalające na rejestrację zdarzeń, zarządzanie konfiguracją agentów oraz odczyt stanu każdego z monitorowanych komponentów.
	Logowanie operatorów do systemu musi odbywać się z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością (SSO) co najmniej w zakresie protokołu SAML2.

	System musi posiadać kontrolę dostępu opartą na rolach (RBAC).
	System musi posiadać funkcję wysyłania powiadomień do użytkowników lub grup w odpowiedzi na występujące zagrożenia. System musi wysyłać powiadomienia co najmniej za pomocą email oraz SMS.
	System musi być dostarczony wraz z wbudowanymi regułami detekcji. Musi istnieć możliwość dodawania własnych reguł.
	System musi umożliwiać zaawansowane metody detekcji poprzez integrację z frameworkiem MITRE ATT&CK.
	System musi wykrywać i aktywnie blokować ataki typu brute-force na hasła systemów operacyjnych.
	System musi umożliwiać integrację z oprogramowaniem NIDS tj. Suricata.
	System musi wykrywać i zapobiegać atakom typu SQL Injection.
	System musi wykrywać i blokować ataki typu DDoS.
	System musi umożliwiać wykrywania i usuwanie malware poprzez integrację z zewnętrznymi bazami i narzędziami tj. VirusTotal.
	System musi wykrywać znane podatności na każdym monitorowanym obiekcie z wykorzystaniem baz CVE.
	System musi wykrywać ukryte procesy oraz wykonywanie podejrzanych operacji przez zainstalowane w systemie operacyjnym monitorowanego obiektu aplikacje.
Agent	System musi udostępniać dedykowane pliki instalacyjne agentów dla systemów co najmniej Windows, Linux oraz MacOS.
	Agent musi komunikować się z serwerem systemu za pomocą szyfrowanego i autoryzowanego połączenia.
	Agent musi posiadać funkcjonalność zdalnej konfiguracji oraz zdalnej aktualizacji po podłączeniu się do serwera.

	Agent musi posiadać budowę modułową z możliwością wyłączenia poszczególnych modułów w zależności od wymaganej konfiguracji oraz możliwości wydajnościowych monitorowanego obiektu.
	Agent musi posiadać co najmniej następujące moduły: • Moduł zbierania logów (kolektor logów) • Moduł wykonywania poleceń • Moduł monitorowania integralności plików • Moduł inwentaryzacji zasobów • Moduł oceny konfiguracji bezpieczeństwa (SCA) • **Moduł wykrywania podatności** • Moduł zgodności ze standardami bezpieczeństwa • Moduł reaktywnej odpowiedzi • Moduł wykrywania malware
	Agent musi posiadać kolektor logów wspierający filtry XPath do przetwarzania Dziennika zdarzeń systemu Windows.
	Kolektor logów musi wspierać odczyt wielolinijkowych logów (co najmniej format Linux Audit).
	Monitor integralności plików musi umożliwiać rejestrowania zdarzeń tj. utworzenie pliku, modyfikacja lub usunięcie wraz ze wskazaniem użytkownika oraz czasu zdarzenia. Dodatkowo moduł musi umożliwiać monitorowanie zmian atrybutów, uprawnień, właściciela oraz monitoring zawartości pliku.
	Moduł inwentaryzacji zasobów musi zbierać i udostępniać informacje o obiekcie w zakresie co najmniej: • Rodzaj i wersja systemu operacyjnego, • Lista i rodzaj interfejsów sieciowych, • Lista aktywnych procesów systemu operacyjnego, • Lista zainstalowanych aplikacji, • Lista otwartych portów sieciowych.
	Moduł oceny konfiguracji bezpieczeństwa musi umożliwiać, za pomocą predefiniowanych reguł, skanowanie obiektu w celu wykrycia zagrożeń lub błędnych konfiguracji w zakresie co najmniej: • Siła haseł, • Usunięcie niepotrzebnego lub niebezpiecznego oprogramowania, • Wyłączenie zbędnych usług

	Moduł musi posiadać predefiniowane reguły SCA dla każdego z wymaganych systemów operacyjnych oraz udostępniać możliwość tworzenia własnych polityk SCA.
	Moduł wykrywania podatności musi umożliwiać wykrywania luk w aplikacjach zainstalowanych na obiekcie za pomocą dostawców tj. National Vulnerability Database, Red Hat, Canonical, ALAS, MSU.
	Moduł zgodności ze standardami bezpieczeństwa musi umożliwiać badania obiektu pod katem zgodności ze standardami tj. PCI DSS, HIPAA, NIST 800-53 oraz GDPR.
	Moduł reaktywnej odpowiedzi musi umożliwiać automatyczne (bez udziału operatora SIEM) uruchomienie akcji tj.: • Zablokowanie połączenia sieciowego, • Zatrzymanie aktywnego procesu, • Usunięcie pliku, • Przeskanowanie pliku pod kątem obecności wirusów.
	Moduł wykrywania malware musi posiadać możliwość wykrywania anomalii i na tej podstawie obecności złośliwego oprogramowania. Moduł musi umożliwiać wykrywania ukrytych procesów, ukrytych plików oraz podejrzanych otwartych portów TCP/UDP.

Integracja z wdrażanym w ramach realizacji przedmiotu zamówienia systemem SIEM została opisana w tabeli.

Obszar	Wymaganie
Bezpieczne przekazywanie danych	Wykonawca zapewni bezpieczny mechanizm przekazywania danych z systemu SIEM Zamawiającego do środowiska SOC Wykonawcy, z wykorzystaniem szyfrowanej komunikacji i uzgodnionych zasad dostępu.
Minimalizacja danych	Zakres przekazywanych danych powinien być ograniczony do informacji niezbędnych do świadczenia usługi SOC, z uwzględnieniem zasady minimalizacji danych.
Agregacja danych	Do środowiska SOC Wykonawcy powinny trafiać dane zagregowane i odfiltrowane, pozwalające na analizę bezpieczeństwa bez nieuzasadnionego

	przekazywania pełnego strumienia logów, jeżeli nie jest to konieczne dla realizacji usługi.
Uzgodnienie źródeł	Zamawiający i Wykonawca uzgodnią listę źródeł logów oraz typów zdarzeń objętych monitoringiem.
Uzgodnienie reguł	Wykonawca uzgodni z Zamawiającym zestaw reguł, filtrów, korelacji i typów alertów, które będą przekazywane do SOC.
Dostępność połączenia	Wykonawca zapewni konfigurację połączenia umożliwiającego regularne przekazywanie zdarzeń do środowiska SOC w czasie umożliwiającym ich analizę w ramach godzin świadczenia usługi.
Ochrona danych	Dane przekazywane do SOC muszą być chronione przed dostępem osób nieuprawnionych, modyfikacją, utratą lub ujawnieniem.
Rozdzielenie środowisk	Środowisko SOC Wykonawcy powinno zapewniać logiczne rozdzielenie danych Zamawiającego od danych innych klientów Wykonawcy.
Retencja danych	Wykonawca określi i uzgodni z Zamawiającym okres retencji danych, raportów i zdarzeń przetwarzanych w ramach usługi SOC.
Poufność	Wykonawca zobowiązany będzie do zachowania poufności wszystkich informacji uzyskanych w związku ze świadczeniem usługi SOC.

Wymagania dotyczące centrum przetwarzania danych SOC:

- Centrum przetwarzania danych, w którym będą składowane wyniesione kopie zapasowe, musi spełniać co najmniej standard TIER III (poziom z pełną redundancją krytycznych systemów i możliwością utrzymania bez przerywania pracy centrum danych, zapewniający wysoką dostępność) lub równoważne.
- Infrastruktura w centrum przetwarzania danych, spełnia co najmniej następujące wymagania:
    - posiada aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
    - musi posiadać redundantne wewnętrzne linie chłodu;
    - musi posiadać możliwość odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynnościom serwisowym, tak aby nie zakłócić normalnej pracy urządzeń dwu-zasilaczowych;
    - musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
    - musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
    - musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenia ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;

- musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
- musi posiadać zasilanie gwarantowane w układzie n+1, zapewniające nieprzerwane zasilanie;
- dystrybucja energii elektrycznej odbywa się z wykorzystaniem niezależnych torów zasilania, z osobnym zabezpieczeniem nadmiarowo prądowym z gwarantowanym podtrzymaniem zasilania z wykorzystaniem UPS i agregatu prądotwórczego;
- podstawowe i zapasowe łącza internetowe symetryczne każde o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury.

Wymagania dotyczące SLA dla usługi:

Priorytet zdarzenia	Charakterystyka	L1: rozpoczęcie analizy	L1: eskalacja	L2: rozpoczęcie analizy	L2: rekomendacja działań
P1 – Krytyczny	Zdarzenie wskazujące na aktywny incydent bezpieczeństwa, możliwe przejęcie konta uprzywilejowanego, ransomware, masową infekcję, eksfiltrację danych lub naruszenie kluczowych systemów.	do 15 min	do 30 min	do 30 min	do 2 h
P2 – Wysoki	Zdarzenie mogące wskazywać na próbę naruszenia bezpieczeństwa, podejrzaną aktywność użytkownika, wykrycie malware, nietypową komunikację sieciową lub istotną anomalię.	do 30 min	do 1 h	do 1 h	do 4 h
P3 – Średni	Zdarzenie wymagające weryfikacji, ale bez bezpośrednich przesłanek aktywnego naruszenia, np. pojedyncze anomalie, podejrzane logowania, błędy konfiguracji, powtarzalne alerty.	do 4 h	do 8 h	do 12 h	do 2 dni roboczych
P4 – Niski	Zdarzenie informacyjne, techniczne lub niskiego ryzyka, wymagające odnotowania, obserwacji albo uwzględnienia w raporcie okresowym.	do 1 dnia roboczego	według zasad raportowania	do 2 dni roboczych	do 5 dni roboczych

Przeprowadzenie szkoleń

Szkolenia z wdrożonego oprogramowania

W ramach realizacji zamówienia Wykonawca zobowiązany jest do przeprowadzenia szkoleń stanowiskowych dla wyznaczonych pracowników Zamawiającego z zakresu obsługi, administracji oraz bieżącego utrzymania wdrożonych rozwiązań informatycznych. Szkolenia będą realizowane przez inżynierów Wykonawcy przy okazji wdrożenia i konfiguracji poszczególnych systemów.

Szkolenia powinny mieć charakter praktyczny i obejmować omówienie podstawowych funkcji administracyjnych, zasad codziennej obsługi, monitorowania stanu systemów, reagowania na alerty i zdarzenia, wykonywania podstawowych czynności utrzymaniowych, tworzenia i odtwarzania kopii zapasowych, zarządzania użytkownikami i uprawnieniami, a także interpretacji logów, komunikatów oraz raportów generowanych przez wdrożone rozwiązania.

Celem szkoleń jest przygotowanie personelu Zamawiającego do samodzielnej eksploatacji wdrożonych systemów po zakończeniu realizacji zamówienia, w zakresie niezbędnym do ich bieżącego utrzymania, podstawowej diagnostyki oraz prawidłowego wykorzystania w procesach zapewnienia ciągłości działania i cyberbezpieczeństwa organizacji.

Szkolenia specjalistyczne z zakresu analizy ruchu sieciowego

Cel szkolenia

Celem szkolenia jest przygotowanie uczestników do monitorowania bezpieczeństwa infrastruktury teleinformatycznej, analizy logów systemowych i sieciowych, identyfikacji incydentów bezpieczeństwa oraz stosowania podstawowych technik hardeningu systemów operacyjnych Windows i Linux. Szkolenie powinno mieć charakter praktyczny i obejmować ćwiczenia laboratoryjne pozwalające na analizę rzeczywistych zdarzeń bezpieczeństwa.

Zakres szkolenia

Moduł 1. Podstawy monitorowania bezpieczeństwa systemów IT

Szkolenie powinno obejmować co najmniej:

- rolę monitorowania w zapewnianiu cyberbezpieczeństwa,
- źródła danych wykorzystywane podczas monitorowania bezpieczeństwa,
- rodzaje logów systemowych i aplikacyjnych,
- podstawowe scenariusze wykrywania incydentów bezpieczeństwa,
- proces monitorowania zdarzeń oraz reagowania na wykryte nieprawidłowości.

Moduł 2. Analiza logów systemów Microsoft Windows

Zakres powinien obejmować co najmniej:

- architekturę logowania zdarzeń w systemie Windows,
- wykorzystanie Windows Event Viewer,
- analizę logów bezpieczeństwa, aplikacji oraz systemowych,
- monitorowanie aktywności użytkowników i procesów,
- identyfikację prób nieautoryzowanego dostępu,
- wykorzystanie podstawowych poleceń PowerShell i CMD wspomagających analizę bezpieczeństwa,
- ćwiczenia laboratoryjne z analizy zdarzeń.

Moduł 3. Analiza logów systemów Linux

Zakres powinien obejmować:

- lokalizację i strukturę logów systemowych,
- analizę logów uwierzytelniania oraz zdarzeń systemowych,

- monitorowanie aktywności użytkowników,
- wykorzystanie podstawowych narzędzi administracyjnych i analitycznych systemu Linux,
- analizę incydentów bezpieczeństwa,
- ćwiczenia praktyczne.

Moduł 4. Analiza ruchu sieciowego

Zakres szkolenia powinien obejmować:

- podstawy komunikacji sieciowej wykorzystywane podczas analizy bezpieczeństwa,
- identyfikację prawidłowego i nieprawidłowego ruchu sieciowego,
- analizę podstawowych protokołów sieciowych,
- przechwytywanie i analizę pakietów,
- wykorzystanie narzędzi do analizy ruchu sieciowego, w szczególności Wireshark oraz tcpdump lub narzędzi równoważnych,
- identyfikację anomalii i prób nieautoryzowanego dostępu,
- ćwiczenia laboratoryjne.

Moduł 5. Hardening systemów operacyjnych

Szkolenie powinno obejmować:

- zasady hardeningu systemów Windows i Linux,
- ograniczanie powierzchni ataku,
- zabezpieczanie usług systemowych,
- konfigurację podstawowych mechanizmów bezpieczeństwa,
- wykorzystanie narzędzi diagnostycznych i sieciowych (m.in. ping, tracert, nslookup, netstat lub narzędzi równoważnych),
- dobre praktyki zabezpieczania stacji roboczych i serwerów.

Moduł 6. Analiza zdarzeń bezpieczeństwa z wykorzystaniem rozwiązań AV/EDR

Zakres powinien obejmować:

- podstawowe funkcje systemów Endpoint Detection and Response (EDR),
- analizę logów generowanych przez rozwiązania AV/EDR,
- identyfikację podejrzanych aktywności,
- korelację zdarzeń bezpieczeństwa,
- interpretację alertów bezpieczeństwa,
- praktyczne scenariusze wykrywania zagrożeń z wykorzystaniem rozwiązania klasy EDR lub równoważnego.

Forma realizacji

Szkolenie powinno:

- mieć charakter praktyczny,
- obejmować laboratoria wykonywane przez uczestników,
- wykorzystywać rzeczywiste scenariusze incydentów bezpieczeństwa,
- zapewniać materiały szkoleniowe w wersji elektronicznej,
- zakończyć się wydaniem imiennego certyfikatu lub zaświadczenia o ukończeniu szkolenia.

Szkolenia dla personelu z zakresu cyberhigieny wraz z testami socjotechnicznymi (usługa security awarness)

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników biurowych Zamawiającego (20 osób). Szkolenie ma na celu podniesienie świadomości użytkowników końcowych w zakresie aktualnych zagrożeń cybernetycznych, metod działania cyberprzestępców oraz zasad bezpiecznego korzystania z systemów informatycznych, poczty elektronicznej, dokumentów, urządzeń i

danych wykorzystywanych w codziennej pracy. Szkolenie będzie zrealizowane w formie zdalnej. Czas szkolenia to minimum 8 godzin zegarowych.

Szkolenie musi obejmować w szczególności zagadnienia dotyczące phishingu, spamu, ataków socjotechnicznych, fałszywych faktur, bezpieczeństwa haseł, uwierzytelniania wieloskładnikowego, aktualizacji oprogramowania, ochrony danych, bezpieczeństwa fizycznego stanowiska pracy, korzystania z nośników zewnętrznych, bezpieczeństwa urządzeń służbowych i prywatnych, zagrożeń związanych z wykorzystaniem sztucznej inteligencji, deepfake oraz zasad weryfikacji podejrzanych dyspozycji lub komunikatów z wykorzystaniem niezależnego kanału komunikacji.

Szkolenie powinno mieć charakter praktyczny i być dostosowane do osób nieposiadających specjalistycznej wiedzy informatycznej. Wykonawca zobowiązany jest do przedstawienia treści w sposób zrozumiały dla pracowników biurowych, z wykorzystaniem przykładów sytuacji występujących w codziennej pracy organizacji. Szkolenie powinno wspierać realizację obowiązków Zamawiającego w zakresie budowania świadomości cyberbezpieczeństwa, ograniczania ryzyka incydentów oraz spełniania wymagań wynikających z aktualnych regulacji i dobrych praktyk bezpieczeństwa, w tym dyrektywy NIS2.

W ramach szkolenia zostanie opracowany i przeprowadzony test phishingowy pozwalający zweryfikować:

- jak pracownicy reagują na realnie wyglądające próby wyłudzenia,
- kto otwiera podejrzane wiadomości,
- kto klika w linki lub pobiera załączniki,
- jakie są potencjalne luki wynikające z czynnika ludzkiego.

Celem testu jest precyzyjna weryfikacja aktualnego poziomu świadomości zespołu oraz wskazanie obszarów wymagających poprawy.

Wykonawca zapewni materiały szkoleniowe, potwierdzenia ukończenia szkolenia dla uczestników oraz dokumentację potwierdzającą realizację usługi. W przypadku szkolenia prowadzonego na żywo Wykonawca zapewni możliwość zadawania pytań oraz omówienia praktycznych przykładów zagrożeń.

Szkolenie musi obejmować co najmniej następujące obszary tematyczne:

Obszar	Minimalny zakres wymagania

Podstawy cyberbezpieczeństwa	Omówienie podstawowych pojęć związanych z cyberbezpieczeństwem, cyberprzestępczością, zagrożeniami sieciowymi oraz rolą użytkownika w systemie bezpieczeństwa organizacji
Aktualny krajobraz zagrożeń	Przedstawienie aktualnych zagrożeń cybernetycznych występujących w Polsce i na świecie, ze szczególnym uwzględnieniem zagrożeń dla pracowników biurowych i instytucji
Ataki na pracowników	Omówienie typowych metod ataków kierowanych do pracowników, w tym phishingu, spamu, fałszywych wiadomości, złośliwych załączników, fałszywych faktur oraz podszywania się pod kontrahentów lub przełożonych
Socjotechnika	Wyjaśnienie mechanizmów manipulacji stosowanych przez cyberprzestępców, w tym wyłudzania danych, presji czasu, fałszywego autorytetu, wzbudzania zaufania oraz wykorzystywania nieuwagi użytkownika
Phishing i kradzież danych	Przedstawienie zasad rozpoznawania wiadomości phishingowych, fałszywych stron logowania, podejrzanych linków i załączników oraz metod ochrony kont służbowych i prywatnych
Bezpieczeństwo faktur i płatności	Omówienie ryzyk związanych z fałszywymi fakturami, zmianą numerów rachunków bankowych, przechwytywaniem korespondencji oraz koniecznością weryfikacji danych płatniczych innym kanałem komunikacji
KSeF i dokumenty elektroniczne	Omówienie ryzyk związanych z obsługą dokumentów elektronicznych, w tym dokumentów finansowych, faktur oraz potencjalnych nadużyć związanych z obiegiem dokumentów
Sztuczna inteligencja w cyberatakach	Omówienie sposobów wykorzystania AI przez cyberprzestępców, w tym generowania wiarygodnych wiadomości, deepfake, fałszywych nagrań głosowych, obrazów, dokumentów i komunikatów
Deepfake i fałszywa tożsamość	Przedstawienie zagrożeń wynikających z podszywania się pod osoby, instytucje lub kontrahentów przy użyciu technologii generatywnych

Weryfikacja dwuetapowa danych	Omówienie procedury weryfikacji użytkowników, dyspozycji, danych płatniczych i nietypowych poleceń z wykorzystaniem co najmniej dwóch niezależnych kanałów komunikacji
Hasła i uwierzytelnianie	Omówienie zasad tworzenia i ochrony silnych haseł, ryzyk związanych z ponownym używaniem haseł, korzyści z menedżerów haseł oraz metod logowania 2FA/MFA
Aktualizacje oprogramowania	Wyjaśnienie znaczenia aktualizacji systemów, aplikacji i urządzeń dla ograniczenia podatności oraz ryzyka przejęcia urządzeń
Botnety i przejęcie urządzeń	Omówienie zagrożeń związanych z przejmowaniem urządzeń przez cyberprzestępców oraz wykorzystaniem ich do dalszych ataków
Ataki DoS/DDoS	Przedstawienie podstawowych informacji o atakach DoS/DDoS oraz ich skutkach dla organizacji i dostępności usług
Bezpieczeństwo fizyczne	Omówienie zasad zabezpieczania stanowiska pracy, dokumentów, ekranów, urządzeń, identyfikatorów, nośników danych i dostępu do pomieszczeń
Nośniki zewnętrzne	Przedstawienie zasad bezpiecznego postępowania z pendrive'ami, dyskami zewnętrznymi, kartami pamięci i innymi nośnikami danych
Sprzęt prywatny i służbowy	Omówienie ryzyk wynikających z używania sprzętu prywatnego do celów służbowych oraz zasad bezpiecznego korzystania z urządzeń firmowych
Kradzież tożsamości	Omówienie ryzyk związanych z ujawnianiem danych osobowych, służbowych i uwierzytelniających oraz sposobów ograniczania skutków kradzieży tożsamości
Reagowanie na incydenty	Przedstawienie zasad zgłaszania podejrzanych wiadomości, incydentów, utraty danych, podejrzenia infekcji lub naruszenia bezpieczeństwa

Wykonawca powinien uwzględnić w szkoleniu wymagania i dobre praktyki wynikające z aktualnych regulacji oraz obowiązków w zakresie cyberbezpieczeństwa (tj NIS2, uKSC 2.0), w szczególności:

Parametr	Wartość wymagania
Zgodność z NIS2	Szkolenie powinno uwzględniać wymagania dyrektywy NIS2 w zakresie budowania świadomości cyberbezpieczeństwa i ograniczania ryzyk organizacyjnych
Bezpieczeństwo informacji	Szkolenie powinno wspierać realizację zasad ochrony informacji, poufności danych, integralności i dostępności usług
Ochrona danych	Program powinien odnosić się do ryzyk związanych z przetwarzaniem danych osobowych i służbowych w codziennej pracy
Świadomość użytkowników	Szkolenie powinno wzmacniać świadomość pracowników jako jednego z kluczowych elementów systemu bezpieczeństwa organizacji
Dobre praktyki organizacyjne	Szkolenie powinno obejmować praktyczne procedury postępowania w przypadku podejrzenia ataku, wycieku danych, fałszywej wiadomości lub próby wyłudzenia

Szkolenia dla kadry zarządzającej (symulacja z zakresu ciągłości działania)

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa strategicznego, przeznaczonego dla kadry kierowniczej, osób zarządzających komórkami organizacyjnymi oraz osób odpowiedzialnych za podejmowanie decyzji organizacyjnych i nadzorczych w obszarze bezpieczeństwa informacji, ciągłości działania oraz zarządzania ryzykiem (razem 2 osoby). Szkolenie będzie zrealizowane w formie zdalnej. Czas szkolenia to minimum 8 godzin zegarowych.

Celem szkolenia jest podniesienie świadomości kadry zarządzającej w zakresie aktualnych zagrożeń cyberbezpieczeństwa, sposobów działania cyberprzestępców, skutków organizacyjnych i finansowych incydentów bezpieczeństwa oraz roli osób decyzyjnych w budowaniu odporności organizacji na cyberataki. Szkolenie powinno koncentrować się nie tylko na aspektach technicznych, lecz przede wszystkim na odpowiedzialności zarządczej, ryzyku operacyjnym, procedurach, komunikacji, organizacji pracy oraz podejmowaniu decyzji w sytuacji incydentu.

Szkolenie powinno zostać przeprowadzone w formule wykładowo-warsztatowej, z wykorzystaniem przykładów praktycznych, studiów przypadków oraz omówienia typowych błędów organizacyjnych popełnianych przez kadrę kierowniczą w obszarze cyberbezpieczeństwa. Zakres szkolenia powinien być dostosowany do osób nietechnicznych lub częściowo technicznych, tak aby umożliwić skuteczne zrozumienie ryzyka cybernetycznego z perspektywy zarządzania organizacją.

Obszar	Wymagany zakres
Aktualny krajobraz zagrożeń	Omówienie aktualnych zagrożeń cyberbezpieczeństwa istotnych dla jednostek organizacyjnych, przedsiębiorstw i instytucji publicznych, w tym motywacji i sposobów działania cyberprzestępców.
Profilowanie celu ataku	Przedstawienie, w jaki sposób atakujący wybierają cele, pozyskują informacje o organizacji, analizują strukturę pracowników, dane publiczne, procesy administracyjne i finansowe.
Ataki na administrację i finanse	Omówienie zagrożeń skierowanych do działów administracyjnych, finansowych, księgowych, sekretariatów oraz osób posiadających uprawnienia decyzyjne lub dostęp do informacji wrażliwych.
Phishing i socjotechnika	Przedstawienie mechanizmów phishingu, spear phishingu, podszywania się pod kontrahentów, przełożonych, instytucje publiczne lub dostawców usług oraz metod ograniczania skuteczności takich ataków.
Wykorzystanie sztucznej inteligencji w cyberatakach	Omówienie wpływu narzędzi AI na jakość i skalę ataków, w szczególności phishingu, automatyzacji rozpoznania, generowania fałszywych treści oraz manipulacji komunikacją.
OPSEC w praktyce	Wyjaśnienie zasad bezpieczeństwa operacyjnego, w tym ograniczania ujawniania informacji o organizacji, pracownikach, infrastrukturze, procesach i planowanych działaniach.

Czynnik ludzki	Omówienie roli pracowników i kadry zarządzającej w systemie bezpieczeństwa, ze szczególnym uwzględnieniem błędów ludzkich, rutyny, presji czasu, braku weryfikacji oraz niewłaściwych nawyków.
Procedury i praktyka działania	Przedstawienie znaczenia procedur bezpieczeństwa, ale także ich praktycznego egzekwowania, testowania, komunikowania i dostosowania do realnych procesów organizacji.
Sprzęt prywatny i służbowy	Omówienie ryzyk związanych z wykorzystywaniem prywatnych urządzeń, pracy zdalnej, dostępem do poczty, systemów wewnętrznych oraz danych organizacji poza kontrolowanym środowiskiem.
Cyberbezpieczeństwo jako ryzyko zarządcze	Przedstawienie cyberbezpieczeństwa jako elementu zarządzania ryzykiem organizacyjnym, a nie wyłącznie zadania działu IT.
Pułapki decyzyjne kadry zarządzającej	Omówienie najczęstszych błędów decyzyjnych, takich jak niedoszacowanie ryzyka, odkładanie działań zabezpieczających, brak właścicieli procesów, pozorna zgodność z procedurami lub nadmierne poleganie na technologii.
KSeF i nowe obszary ryzyka	Omówienie ryzyk związanych z cyfryzacją procesów finansowo-księgowych, w tym zmianami organizacyjnymi, dostępami, uprawnieniami i ciągłością działania w kontekście systemów takich jak KSeF.
Rola kadry kierowniczej w reagowaniu na incydenty	Przedstawienie odpowiedzialności osób zarządzających podczas incydentu, w tym w zakresie eskalacji, komunikacji, podejmowania decyzji, dokumentowania działań i współpracy z zespołami technicznymi.
Budowanie odporności organizacji	Omówienie działań organizacyjnych zwiększających odporność na cyberataki, w tym szkoleń, testów, procedur, segmentacji odpowiedzialności, planów awaryjnych i regularnej weryfikacji zabezpieczeń.
Sesja pytań i odpowiedzi	Zapewnienie czasu na omówienie pytań uczestników oraz odniesienie omawianych zagadnień do realiów organizacji Zamawiającego.

Audyty zgodności SZBI i SZCD

Przedmiotem zadania jest przeprowadzenie audytu SZBI, audytu SZCD, audytu zgodności z KRI/UoKSC. Zakres taki odpowiada praktyce rynkowej i zakresom wskazywanym w materiałach dotyczących programu, obejmującym audyty zgodności, audyty SZBI/SZCD oraz elementy związane z IT/OT/ICS.

Audyty zostaną przeprowadzone przez osoby posiadające odpowiednie kwalifikacje i doświadczenie oraz legitymujące się odpowiednim certyfikatem audytora wiodącego dla norm ISO27001 oraz ISO22301.

Wykonawca zobowiązany jest zapewnić pełną niezależność i bezstronność osób realizujących audyt SZBI oraz SZCD. Audyt nie może być przeprowadzany przez osoby, które brały udział w opracowaniu, wdrożeniu lub konfiguracji dokumentacji, procedur, systemów lub rozwiązań objętych przedmiotem zamówienia. Wykonawca zobowiązany jest on do organizacyjnego rozdzielenia zespołu wdrożeniowego od zespołu audytowego oraz zapewnienia, że osoby wykonujące audyt będą wolne od konfliktu interesów i zachowają pełną obiektywność podczas oceny zgodności wdrożonych rozwiązań z wymaganiami obowiązujących przepisów, norm oraz dokumentacji projektowej. Na żądanie Zamawiającego Wykonawca przedstawi oświadczenia o bezstronności i braku konfliktu interesów osób wyznaczonych do realizacji audytu.

W ramach zadania Wykonawca zobowiązany będzie co najmniej do:

- przygotowania programu i planu audytu,
- przeglądu dokumentacji,
- przeprowadzenia wywiadów i czynności weryfikacyjnych,
- oceny zgodności z wymaganiami wskazanymi przez Zamawiającego,
- oceny skuteczności wdrożonych rozwiązań,
- sporządzenia raportu audytowego zawierającego niezgodności, obserwacje i rekomendacje,
- przedstawienia wyników audytu Zamawiającemu podczas spotkania podsumowującego.

W wyniku realizacji zadania Wykonawca przekaże co najmniej:

- plan audytu,

- listy kontrolne lub równoważne narzędzia oceny,
- raport lub raporty audytowe,
- rejestr stwierdzonych niezgodności i obserwacji,
- rekomendacje działań korygujących i doskonalących.

Za wykonane prawidłowo uznaje się zadanie, jeżeli:

- audyt został przeprowadzony według uzgodnionego planu,
- raport przedstawia jednoznaczne ustalenia i podstawę oceny,
- ustalenia zostały przyporządkowane do odpowiednich wymagań lub kryteriów audytu,
- Zamawiający otrzymał rekomendacje możliwe do wykorzystania w działaniach naprawczych i doskonalących.