Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa postępowania: Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Zakład Usług Wodnych i Komunalnych Sp. z o. o. z siedzibą w Strzelcach w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo - CyberPL" - Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności.

Przeprowadzenie audytu, szkoleń oraz dostawa sprzętu, usług i oprogramowania w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności.

Postępowanie nr 2/KPO/2026

Spis treści

Preambuła....4

1. Oprogramowanie do badania podatności systemów informatycznych – 1 komplet....6
2. Oprogramowanie do ochrony przed ransomware – 1 komplet....7
3. Oprogramowanie typu EDR (Endpoint Detection and Response) – 1 komplet....15
4. Oprogramowanie typu NDR – 1 szt....19
5. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IoT....20
6. NGFW (Next Gen FireWall) – 2 szt....21
7. Usługa konfiguracji i hardening systemów/urządzeń IT/OT/ICS/IIoT....27
8. Stacja robocza fizyczna lub wirtualna z rolą stacji przesiadkowej – 2 szt....28
9. Usługa segmentacji sieci IT/OT/ICS/IIoT....34
10. Network Attached Storage (NAS) – 2 szt....35
11. System operacyjny i/lub licencje dostępowe (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 1 komplet....37
12. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 1szt....39

13. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 1szt. 41
14. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa. 43
15. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X(Switch) – 1 komplet 44
16. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 1 szt 46
17. Oprogramowanie typu ITSM – 1 szt 48
18. Oprogramowanie typu MDM – 1 szt 49
19. Ochrona AntyDDos system typu DLP – 2 komplety 50
20. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT. – 1 komplet. 52
21. Oprogramowanie do zarządzania tożsamością i dostępem. 54
22. Oprogramowanie typu MFA (dwu/wieloskładniwe uwierzytelnienie). – 6 szt. 56
23. Klucze sprzętowe U2F – 1 szt. 57
24. Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych) typ 1 - 2szt 58
25. Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych) typ 2 – 3szt 60
26. Oprogramowanie/licencje IDS dedykowane sieciom OT — 1 szt. 61
27. UTM (Unified Threat Management) – 1szt. 63
28. Usługa Private APN – 5 szt 68
29. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 1szt. 69
30. Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT 70
31. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IoT 71
32. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu OpenSource IT/OT/ICS/IIoT 72
33. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT 76
34. Szkolenie z zakresu Cyberbezpieczeństwo – szkolenie specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowana) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS 77
35. Szkolenia z zakresu cyberbezpieczeństwa kadry, istotnych z punktu widzenia wdrażanej Polityki Bezpieczeństwa Informacji i Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). 78

36. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, weryfikującymi świadomość zagrożeń i reakcje personelu, w szczególności osób realizujących obowiązki w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z przyjętymi procedurami 79

37. Audyt cyberbezpieczeństwa sieci OT/IT/ICS/IIOT 81

Preambuła

Zamawiający realizuje zadania związane z zapewnieniem ciągłości usług zbiorowego zaopatrzenia w wodę oraz odprowadzania ścieków. Usługi te mają fundamentalne znaczenie dla bezpieczeństwa mieszkańców, ochrony zdrowia publicznego, ochrony środowiska naturalnego, funkcjonowania administracji publicznej, przedsiębiorstw oraz ciągłości działania infrastruktury technicznej państwa.

Współczesne systemy wodociągowe i kanalizacyjne są w znacznym stopniu zależne od systemów teleinformatycznych, systemów automatyki przemysłowej, systemów sterowania, systemów monitorowania procesów technologicznych oraz systemów komunikacyjnych. Cyberatak, lub awaria tych systemów może prowadzić do zakłócenia procesów technologicznych, ograniczenia zdolności świadczenia usług publicznych, utraty integralności danych, szkód środowiskowych, strat ekonomicznych, a w skrajnych przypadkach również do zagrożenia zdrowia i życia ludzi.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej wskazuje, że jednym z podstawowych celów państwa jest zwiększenie odporności podmiotów publicznych i gospodarczych na zagrożenia cyberbezpieczeństwa, zwiększenie zdolności do wykrywania zagrożeń i reagowania na incydenty, wzmacnianie bezpieczeństwa łańcucha dostaw oraz wzmacnianie suwerenności technologicznej Rzeczypospolitej Polskiej. Dokument ten wskazuje również, że zapewnienie bezpieczeństwa usług niezbędnych dla funkcjonowania społeczeństwa i gospodarki wymaga wdrażania adekwatnych środków organizacyjnych, technicznych i proceduralnych służących ograniczaniu ryzyka cybernetycznego.

Zamawiający wskazuje, że cyberbezpieczeństwo nie stanowi wyłącznie zagadnienia technicznego, lecz jest jednym z podstawowych elementów zapewnienia ciągłości realizacji usług publicznych. W związku z tym wszystkie rozwiązania objęte niniejszym postępowaniem muszą być oceniane nie tylko pod względem funkcjonalnym, lecz również pod względem ich wpływu na poziom bezpieczeństwa, odporności operacyjnej, możliwości realizacji obowiązków wynikających z przepisów prawa oraz zdolności do ochrony procesów technologicznych i biznesowych realizowanych przez Zamawiającego.

Przedmiot zamówienia obejmuje budowę, rozbudowę oraz integrację systemu cyberbezpieczeństwa obejmującego środowiska IT oraz OT. Celem projektu jest osiągnięcie zdolności do skutecznego

zapobiegania zagrożeniom, wykrywania incydentów cyberbezpieczeństwa, analizowania ich przyczyn, ograniczania skutków incydentów oraz zapewnienia możliwości odtworzenia przebiegu zdarzeń dla potrzeb działań operacyjnych, audytowych, kontrolnych oraz dowodowych.

Zamawiający przyjmuje zasadę, że bezpieczeństwo środowisk IT i OT powinno być realizowane w sposób zapewniający pełną kontrolę nad procesami bezpieczeństwa, możliwość niezależnej oceny ryzyka, możliwość samodzielnego podejmowania decyzji dotyczących ochrony zasobów oraz możliwość weryfikacji działania zastosowanych środków bezpieczeństwa.

Wszystkie rozwiązania objęte przedmiotem zamówienia muszą wspierać realizację obowiązków wynikających z przepisów prawa krajowego i unijnego dotyczących cyberbezpieczeństwa, ochrony informacji, ciągłości działania oraz zarządzania ryzykiem. Rozwiązania te muszą umożliwiać Zamawiającemu identyfikowanie zagrożeń, monitorowanie stanu bezpieczeństwa, wykrywanie incydentów, prowadzenie analiz bezpieczeństwa, zabezpieczanie materiału dowodowego, realizację obowiązków sprawozdawczych oraz wdrażanie działań naprawczych i doskonalących.

Wymagania określone w dalszej części Opisu Przedmiotu Zamówienia należy traktować jako wymagania minimalne, których spełnienie jest niezbędne do osiągnięcia zakładanych celów projektu, zapewnienia odpowiedniego poziomu cyberodporności oraz ochrony systemów

1. Oprogramowanie do badania podatności systemów informatycznych – 1 komplet

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Instalacja oprogramowania do skanowania, badania i zarządzania podatnościami, np. typu open source, w środowisku serwerowym Zamawiającego.	
2	Konfiguracja podstawowych parametrów systemowych rozwiązania, w tym adresacji IP, DNS oraz synchronizacji czasu NTP.	
3	Konfiguracja dostępu administracyjnego do konsoli zarządzającej systemu.	
4	Konfiguracja ról, uprawnień oraz grup użytkowników administracyjnych w systemie.	
5	Konfiguracja aktualizacji baz testów podatności, definicji podatności, sygnatur lub feed'ów bezpieczeństwa dostępnych dla oferowanego rozwiązania.	
6	Konfiguracja zakresów skanowania wskazanych przez Zamawiającego, obejmujących wybrane zasoby IT,	
7	Zakres: Minimum 7 stacji roboczych Zamawiającego.	

2. Oprogramowanie do ochrony przed ransomware – 1 komplet

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Ochrona antywirusowa musi być monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.	
2	Od strony środowiska Zamawiającego nie może być wymagana instalacja dodatkowych elementów, takich jak baza danych, serwer HTTP czy serwer proxy. Do prawidłowego działania systemu wymagana może być jedynie instalacja agenta na chronionych urządzeniach, łączącego się z centralną konsolą producenta.	
3	System musi umożliwiać instalację agenta ochrony antymalware na wspieranych systemach operacyjnych co najmniej z rodzin: - Microsoft Windows 10 - Microsoft Windows 11 - Microsoft Windows Server 2016 lub nowszy. - macOS.	
4	Wszystkie chronione platformy muszą być zarządzane z tej samej konsoli zarządzającej. Dopuszcza się różnice w zakresie funkcjonalności wynikające z ograniczeń danej platformy.	
5	Konsola zarządzająca musi być obsługiwana co najmniej przez następujące przeglądarki internetowe: - Microsoft Edge, - Mozilla Firefox, - Google Chrome, - Safari.	
6	Konsola zarządzająca oraz oprogramowanie do ochrony stacji roboczych i serwerów muszą posiadać interfejs w języku polskim. Konsola musi dodatkowo obsługiwać co najmniej języki: angielski, niemiecki, francuski, hiszpański, fiński i włoski.	
7	Ten sam agent zainstalowany na systemach Windows musi umożliwiać rozbudowę funkcjonalności o system EDR oraz mechanizm zarządzania ekspozycją na atak. Aktywacja dodatkowych funkcji musi być uzależniona wyłącznie od posiadanej licencji, następować automatycznie po jej dodaniu i nie może wymagać reinstalacji agenta ani osobnej konsoli zarządzającej.	
8	Ochrona antywirusowa musi być realizowana na wielu poziomach, co najmniej przez: - monitor kontrolujący system w tle, - moduł skanowania heurystycznego, - moduł skanujący nośniki wymienne, - monitor ruchu HTTP, - moduł wykrywający rootkity.	
9	System musi posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.	
10	System musi wspierać technologię Antimalware Scan Interface (AMSI).	
11	System musi umożliwiać wybór plików do skanowania – wszystkich plików lub	

	tylko plików o określonych rozszerzeniach – oraz wykluczanie wskazanych rozszerzeń ze skanowania.	
12	System musi umożliwiać ręczną reakcję na wykryte zagrożenie, w tym co najmniej: - wyleczenie pliku, - usunięcie, - przeniesienie do kwarantanny, - zmianę nazwy, - zablokowanie.	
13	System musi chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.	
14	System musi umożliwiać skanowanie dysków sieciowych – dla dowolnych operacji na tych zasobach lub tylko przy uruchamianiu znajdujących się tam plików.	
15	System musi umożliwiać tworzenie wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, co najmniej dla plików, folderów i procesów.	
16	System musi posiadać mechanizm ochrony ruchu HTTP chroniący użytkownika przed złośliwym oprogramowaniem oraz phishingiem, z możliwością wykluczenia wskazanej aplikacji ze skanowania ruchu HTTP.	
17	Aktualizacje baz definicji wirusów muszą być dostępne 24 godziny na dobę na serwerze producenta. System musi umożliwiać aktualizację automatyczną oraz na żądanie, wywoływaną z lokalnego interfejsu oprogramowania.	
18	Aktualizacje definicji wirusów muszą posiadać podpis cyfrowy gwarantujący, że pliki nie zostały zmienione.	
19	System musi umożliwiać dystrybucję aktualizacji baz definicji wirusów oraz oprogramowania na stacjach końcowych za pośrednictwem serwera pośredniczącego.	
20	Aktualizacja oprogramowania klienta do nowej wersji musi następować automatycznie, w sposób niewidoczny dla użytkownika i bez dodatkowych czynności konfiguracyjnych ze strony administratora, w momencie udostępnienia aktualizacji przez producenta.	
21	System musi umożliwiać wywołanie aktualizacji oprogramowania klienta z centralnej konsoli według harmonogramu ustalonego przez administratora dla określonych grup klientów, w tym w określone dni i godziny tygodnia i miesiąca.	
22	System musi umożliwiać wywołanie skanowania na żądanie lub według harmonogramu ustalonego przez administratora dla określonych grup klientów – z centralnej konsoli lub lokalnie na stacji.	
23	System musi umożliwiać uruchamianie skanowania w określone dni i godziny tygodnia i miesiąca oraz po określonym czasie bezczynności komputera.	
24	System musi umożliwiać uruchomienie skanowania z niskim priorytetem, wykorzystującego mniejszą ilość zasobów systemowych.	
25	Aktualizacja definicji wirusów lub mechanizmów skanujących nie może wymagać zatrzymania procesu skanowania.	
26	System musi umożliwiać skanowanie na żądanie pojedynczych plików, katalogów i napędów za pomocą skrótu w menu kontekstowym.	
27	System musi pobierać aktualizacje definicji wirusów i mechanizmów skanujących w sposób przyrostowy (inkrementalny), bez konieczności pobierania całej bazy.	
28	Aktualizacja mechanizmów skanujących i definicji wirusów nie może wymagać restartu systemu operacyjnego.	
29	System musi posiadać heurystyczną technologię wykrywania nowych, nieznanych wirusów.	

30	System musi wykrywać oraz umożliwiać umieszczenie w kwarantannie niepożądanych aplikacji, takich jak: spyware, adware, keylogger, dialer, trojan, rootkit.	
31	System musi posiadać mechanizm wykrywania nowych i nieznanych zagrożeń (0-day) oparty na technologii chmurowej, bazujący w głównej mierze na metadanych analizowanego pliku.	
32	System musi umożliwiać automatyczne przesyłanie podejrzanych plików do środowiska sandbox w infrastrukturze producenta w celu przeprowadzenia dodatkowej analizy strukturalnej i behawioralnej.	
33	System musi umożliwiać wyłączenie automatycznego przesyłania podejrzanych plików do analizy przez producenta.	
34	System musi obsługiwać pliki skompresowane w co najmniej następujących formatach: ZIP, JAR, ARJ, LZH, TAR, TGZ, GZ, CAB, RAR, BZ2.	
35	System musi rejestrować historię działań podejmowanych wobec wykrytych zagrożeń. Dostęp do logów musi być możliwy z poziomu interfejsu aplikacji na stacji oraz z konsoli centralnej.	
36	System musi automatycznie powiadamiać użytkowników oraz administratora o wykrytych zagrożeniach, wraz z informacją, czy stacja jest odpowiednio zabezpieczona. Administrator musi mieć możliwość wyłączenia powiadomień dla użytkowników stacji końcowych.	
37	System musi umożliwiać wyłączenie interfejsu użytkownika oprogramowania na stacji końcowej.	
38	System musi umożliwiać blokowanie określonego przez administratora rodzaju zawartości oraz nazw lub rozszerzeń plików pobieranych za pomocą protokołu HTTP.	
39	System musi umożliwiać wyłączenie skanowania HTTP i blokowania zawartości dla witryn uznanych za zaufane przez system reputacyjny producenta.	
40	System musi umożliwiać instalację dodatku do przeglądarek internetowych (co najmniej Google Chrome, Mozilla Firefox, Microsoft Edge), wyświetlającego graficzną informację o reputacji witryn w wynikach wyszukiwania.	
41	System musi zapewniać ochronę podczas przeglądania Internetu na podstawie reputacji witryn.	
42	System musi umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez producenta – co najmniej 30 kategorii – zarówno dla protokołu HTTP, jak i HTTPS.	
43	Przy próbie wejścia na witrynę z kategorii zablokowanej przez administratora użytkownik musi zostać powiadomiony o blokadzie komunikatem w przeglądarce.	
44	System musi posiadać mechanizm ochrony połączeń z witrynami sklasyfikowanymi jako bankowość elektroniczna, który w czasie trwania sesji co najmniej: - blokuje uruchamianie poleceń cmd oraz skryptów na chronionym hoście, - blokuje zdalny dostęp do hosta za pomocą narzędzi takich jak pulpit zdalny, TeamViewer, LogMeIn, VNC, - czyści zawartość schowka systemowego po zakończeniu sesji.	
45	Administrator musi mieć możliwość objęcia ochroną połączenia dowolnej witryny HTTPS poprzez utworzenie własnej listy takich witryn.	
46	System musi umożliwiać zarządzanie zaporą sieciową wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa przypisywanych do pojedynczych stacji lub grup. Profile muszą zawierać predefiniowane reguły umożliwiające komunikację w sieci lokalnej.	
47	System musi umożliwiać tworzenie własnych reguł zapory co najmniej w oparciu	

	o kierunek komunikacji, protokół sieciowy oraz akcję zezwolenia lub zablokowania.	
48	System musi umożliwiać automatyczne przełączenie profilu zapory po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej).	
49	System musi umożliwiać utworzenie zestawów reguł blokujących komunikację sieciową w celu izolacji hosta na żądanie administratora.	
50	System musi posiadać mechanizm zarządzania aktualizacjami (patch management), umożliwiający instalację poprawek dla systemu operacyjnego oraz zainstalowanych aplikacji, niewymagający instalacji dodatkowych agentów poza agentem ochrony.	
51	Moduł zarządzania aktualizacjami musi okresowo skanować aplikacje zainstalowane na stacji i umożliwiać ich aktualizację do najnowszych wersji – musi pełnić rolę mechanizmu łatającego podatności, a nie jedynie pasywnego skanera.	
52	Administrator musi mieć możliwość określenia, kiedy i jakie aktualizacje mają być instalowane automatycznie.	
53	Administrator musi mieć możliwość uruchomienia na żądanie aktualizacji systemu operacyjnego i aplikacji dla wybranych lub wszystkich hostów.	
54	Mechanizm aktualizacji musi umożliwiać wyświetlenie użytkownikowi komunikatu o konieczności zamknięcia aplikacji w celu dokończenia jej aktualizacji.	
55	W przypadku aktualizacji wymagającej restartu administrator musi mieć możliwość: - wymuszenia automatycznego restartu, - wymuszenia restartu po określonej liczbie godzin, - wyświetlenia użytkownikowi komunikatu o konieczności restartu.	
56	Konsola zarządzająca musi umożliwiać zapoznanie się z opisem podatności aplikacji poprzez odnośnik do strony producenta aplikacji.	
57	Mechanizm aktualizacji nie może wymagać uprawnień administratora lokalnego do instalacji poprawek i musi być realizowany jako dedykowany proces.	
58	Administrator musi mieć możliwość zdefiniowania w konsoli listy aplikacji wykluczonych z aktualizacji.	
59	System musi umożliwiać wyświetlenie w interfejsie na chronionym hoście informacji o brakujących poprawkach systemu i aplikacji oraz ich instalację przez użytkownika.	
60	Konsola zarządzająca musi prezentować listę nieaktualnych aplikacji dla wszystkich chronionych hostów oraz dla pojedynczej stacji.	
61	System musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych, co najmniej: - pamięci masowych, - napędów CD/DVD, - modemów, - portów COM i LPT, - drukarek, - czytników kart pamięci, - kamer, - urządzeń Bluetooth.	
62	System musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane, tworzonej co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.	
63	System musi umożliwiać blokadę zapisu na zewnętrznych dyskach USB (tryb	

	tylko do odczytu).	
64	System musi umożliwiać blokadę uruchamiania plików wykonywalnych z nośników pamięci, przy zachowaniu dostępu do pozostałych danych na nośniku.	
65	System musi umożliwiać zabezpieczenie hasłem możliwości deinstalacji agenta przez użytkownika końcowego.	
66	Administrator musi mieć możliwość wskazania w profilu, które funkcje (lub całość konfiguracji) mogą być zmieniane przez użytkownika na chronionym hoście, oraz zablokowania pozostałych ustawień przed modyfikacją.	
67	System musi posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez ransomware, wykorzystujący własną technologię producenta (a nie np. Volume Shadow Copy Service).	
68	Po wykryciu działania ransomware moduł musi zablokować aktywność szkodliwego procesu oraz przywrócić zaszyfrowane pliki do oryginalnej postaci i lokalizacji.	
69	Moduł przywracania plików musi umożliwiać pracę w trybie monitorowania, bez podejmowania reakcji.	
70	Administrator musi mieć możliwość wskazania własnego folderu na kopie zapasowe plików oraz określenia maksymalnego rozmiaru pliku objętego kopią.	
71	System musi posiadać dodatkowy moduł ochrony danych użytkownika przed ransomware, działający niezależnie od pozostałych modułów, ograniczający możliwość modyfikacji chronionych plików wyłącznie do procesów systemowych i zaufanych aplikacji.	
72	Moduł dodatkowej ochrony przed ransomware musi umożliwiać pracę w trybie monitorowania (bez blokowania), z przekazywaniem administratorowi informacji o próbach modyfikacji plików w chronionych folderach.	
73	Administrator musi mieć możliwość zdefiniowania dodatkowych chronionych folderów zawierających wrażliwe dane użytkownika.	
74	System musi umożliwiać zdefiniowanie zaufanych folderów, z których uruchamiane aplikacje mogą modyfikować pliki objęte dodatkową ochroną przed ransomware.	
75	System musi automatycznie wykrywać zaufane aplikacje, którym zezwala się na dostęp do plików w chronionych folderach, oraz umożliwiać administratorowi ręczne wskazanie zaufanych aplikacji.	
76	System musi posiadać funkcję kontroli uruchamianych aplikacji, umożliwiającą pracę w trybach: - uruchamianie wszystkich aplikacji, - uruchamianie i monitorowanie wszystkich aplikacji, - blokowanie niezaufanych aplikacji.	
77	Kontrola aplikacji musi umożliwiać blokowanie, zezwalanie lub monitorowanie aplikacji co najmniej w oparciu o: - identyfikator SHA-1 i SHA-256, - lokalizację pliku, - wersję pliku, - nazwę aplikacji, - wielkość pliku, - wydawcę, - ważność podpisu cyfrowego.	
78	Reguły kontroli aplikacji muszą obejmować co najmniej czynności: uruchomienie aplikacji, ładowanie modułu, uruchomienie instalatora, dostęp do pliku.	
79	Na wspieranych systemach Windows system musi umożliwiać zdalne	

	uruchomienie szyfrowania dysków za pomocą wbudowanej funkcji BitLocker, z możliwością wymuszenia na użytkowniku ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN.	
80	System musi przekazywać do konsoli zarządzającej klucze odzyskiwania funkcji BitLocker.	
81	System musi umożliwiać zdalne uruchomienie deszyfrowania wcześniej zaszyfrowanych dysków systemowych.	
82	Konsola zarządzająca musi prezentować informacje o stanie zaszyfrowania dysków systemowych.	
83	System musi umożliwiać pobieranie do konsoli informacji z dziennika zdarzeń systemu Windows, co najmniej o: - wyczyszczeniu dziennika audytu, - zablokowaniu konta użytkownika, - utworzeniu i zmianie konta użytkownika, - błędnych próbach logowania, - wystąpieniu błędu krytycznego (BSOD).	
84	Administrator musi mieć możliwość wyboru, które informacje z dziennika zdarzeń systemu Windows są przekazywane do konsoli zarządzającej.	
85	System musi umożliwiać wygenerowanie pliku połączenia zdalnego Microsoft RDP do chronionego hosta, możliwego do wykorzystania w kliencie Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych zgodnych aplikacjach.	
86	Logowanie do konsoli zarządzającej musi umożliwiać wykorzystanie uwierzytelniania wieloskładnikowego (2FA), co najmniej za pomocą powiadomień SMS oraz jednorazowych kodów generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).	
87	Komunikacja pomiędzy konsolą zarządzającą a chronionymi urządzeniami musi być szyfrowana.	
88	Konsola zarządzająca musi wyświetlać powiadomienia o zbliżającym się wygaśnięciu oraz o wygaśnięciu licencji.	
89	Konsola zarządzająca musi posiadać panel kontrolny z podsumowaniem stanu bezpieczeństwa organizacji w postaci interaktywnych wykresów, umożliwiających przejście do szczegółowych danych.	
90	Konsola musi posiadać dedykowaną zakładkę z listą wszystkich chronionych hostów, zawierającą co najmniej nazwę, status ochrony i przypisany profil, z możliwością eksportu listy do pliku CSV.	
91	Szczegóły hosta w konsoli muszą zawierać co najmniej informacje o: - ostatnim połączeniu z konsolą, - wersji zainstalowanego oprogramowania, - systemie operacyjnym, - stanie ochrony, - działaniach związanych z wykrytymi zagrożeniami i skanowaniami.	
92	Z poziomu szczegółów hosta administrator musi mieć możliwość co najmniej: - uruchomienia skanowania antywirusowego, - instalacji aktualizacji systemu operacyjnego i aplikacji, - przypisania profilu, - usunięcia urządzenia, - zmiany klucza subskrypcji, - izolacji hosta od sieci, - pobrania pliku diagnostycznego.	
93	System musi umożliwiać automatyczne usuwanie z listy urządzeń, które nie	

	komunikują się z konsolą, po czasie określonym przez administratora (z możliwością ustawienia co najmniej 60 dni).	
94	Konsola musi posiadać zakładkę z informacjami o brakujących aktualizacjach systemu operacyjnego i aplikacji, z możliwością sortowania i filtrowania według poziomu krytyczności oraz informacją o liczbie i typie hostów, na których brakuje danej poprawki.	
95	Administrator musi mieć możliwość instalacji wskazanej poprawki na wybranych hostach lub na wszystkich hostach, dla których została wydana.	
96	Administrator musi mieć wgląd w historię instalowanych poprawek na chronionych hostach.	
97	System musi posiadać moduł raportowania prezentujący co najmniej stan ochrony, infekcje złośliwym oprogramowaniem oraz zainstalowane aplikacje. Raporty muszą być generowane według harmonogramu i wysyłane na wskazane adresy e-mail.	
98	Konsola musi posiadać mechanizm zarządzania subskrypcjami z możliwością dodawania kluczy licencyjnych oraz prezentować informacje o produkcie, kluczu licencyjnym, typie licencji, wykorzystaniu i dacie wygaśnięcia.	
99	Konsola musi umożliwiać dodawanie kluczy licencyjnych innych produktów producenta, co najmniej dla systemu EDR, zarządzania podatnościami oraz ochrony usług Microsoft 365. Dodanie klucza musi aktywować dedykowaną zakładkę danego produktu w konsoli.	
100	System musi umożliwiać definiowanie profili ustawień dla chronionych urządzeń, przypisywanych do pojedynczych hostów lub grup.	
101	Profile muszą być automatycznie przypisywane do hostów spełniających określone warunki, co najmniej: adres IP, DNS, nazwa WINS, przynależność do Active Directory. Przy automatycznym przypisaniu system musi umożliwiać automatyczne dodanie tagów do hostów.	
102	System musi umożliwiać porównanie dwóch profili konfiguracyjnych w celu wyświetlenia różnic.	
103	Konsola musi umożliwiać pobranie plików instalacyjnych agenta w formatach odpowiednich dla danej platformy, co najmniej: .EXE, .MSI, .MPKG, .DEB, .RPM.	
104	Administrator musi mieć możliwość wyświetlenia dodatkowych szczegółów o chronionych hostach – do wyboru ponad 100 informacji, w tym co najmniej: - wersja BIOS, - identyfikator CPU, - liczba rdzeni procesora, - wolne miejsce na dysku, - informacja o używaniu systemu Windows, który osiągnął koniec wsparcia (end of life), - aktywny wygaszacz ekranu, - zalogowane konto administracyjne.	
105	Konsola musi umożliwiać zarządzanie ochroną urządzeń mobilnych (smartfonów) po wykupieniu odpowiedniej licencji.	
106	Konsola musi umożliwiać tworzenie wielu kont administratorów o różnych poziomach dostępu.	
107	System musi umożliwiać przenoszenie licencji w ramach danego klucza subskrypcji z jednego urządzenia na inne.	
108	Konsola musi posiadać wbudowane narzędzie, wykorzystujące mechanizmy sztucznej inteligencji, do generowania podsumowania zdarzeń bezpieczeństwa z ostatnich 7 dni, w języku konsoli. Korzystanie z narzędzia nie może wymagać	

	dodatkowej licencji.	
109	Wykonawca dostarczy licencję (subskrypcję) systemu ochrony stacji końcowych obejmującą wszystkie funkcje opisane w niniejszej tabeli dla co najmniej 10 urządzeń wraz z prawem do aktualizacji, poprawek oraz wsparcia technicznego przez okres minimum 12 miesięcy.	
110	Usługi wdrożenia: - Konfiguracja konta organizacji Zamawiającego w konsoli zarządzającej oraz kont administratorów z uwierzytelnianiem wieloskładnikowym. - Instalacja i konfiguracja agentów na 7 urządzeniach. - Konfiguracja profili bezpieczeństwa.	

3. Oprogramowanie typu EDR (Endpoint Detection and Response) – 1 komplet

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	System musi obsługiwać co najmniej następujące systemy operacyjne: - Microsoft Windows 10 - Microsoft Windows 11 - Microsoft Windows Server 2016 lub nowszy - macOS w wersjach wspieranych przez producenta systemu operacyjnego	
2	System EDR musi być zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.	
3	Od strony środowiska Zamawiającego nie może być wymagana instalacja dodatkowych elementów, takich jak baza danych, serwer HTTP czy serwer proxy. Do prawidłowego działania systemu wymagana może być jedynie instalacja agenta na chronionych urządzeniach, łączącego się z centralną konsolą producenta.	
4	Ten sam agent zainstalowany na systemach Windows musi umożliwiać rozbudowę funkcjonalności o system ochrony stacji końcowych (EPP) oraz mechanizm zarządzania ekspozycją na atak. Aktywacja dodatkowych funkcji musi być uzależniona wyłącznie od posiadanej licencji, następować automatycznie po jej dodaniu i nie może wymagać reinstalacji agenta ani osobnej konsoli zarządzającej.	
5	Konsola zarządzająca oraz interfejs agenta instalowanego na stacjach końcowych i serwerach muszą być dostępne w języku polskim.	
6	Pomoc i dokumentacja systemu muszą być dostępne co najmniej w języku angielskim.	
7	Agent musi umożliwiać współpracę z oprogramowaniem antywirusowym innych producentów zainstalowanym na stacjach końcowych i serwerach.	
8	Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.	
9	Agent musi umożliwiać instalację z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory (GPO).	
10	Agent musi umożliwiać ręczną instalację, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.	
11	Aktualizacja oprogramowania agenta na stacjach końcowych i serwerach nie może wymagać restartu systemu operacyjnego.	
12	Dane zebrane przez agenta muszą być przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta w celu wykrywania niebezpiecznych zdarzeń.	
13	Agent musi monitorować i zbierać informacje na temat co najmniej następujących zdarzeń: - dostęp do pliku, - tworzenie nowego procesu, - nawiązane połączenia sieciowe, - wpisy dziennika systemu niezbędne do wykrycia naruszeń bezpieczeństwa, - zawartość skryptów uruchamianych na monitorowanej stacji.	
14	W celu zmniejszenia obciążenia stacji końcowych analiza zebranych danych oraz	

	wykrywanie podejrzanych zdarzeń muszą odbywać się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji.	
15	Dane zbierane przez agenta muszą być kompresowane przed wysłaniem do centrum przetwarzania danych, w celu optymalizacji wykorzystania łączy sieciowych.	
16	Komunikacja agentów z centrum przetwarzania danych producenta musi odbywać się wyłącznie z wykorzystaniem protokołów HTTP oraz HTTPS.	
17	Agent musi obsługiwać komunikację za pośrednictwem serwera pośredniczącego HTTP (HTTP proxy).	
18	W przypadku braku dostępu stacji do sieci Internet dane zebrane przez agenta muszą być buforowane lokalnie i przesłane do analizy niezwłocznie po odzyskaniu połączenia.	
19	Dane zbierane przez agentów muszą być przechowywane i przetwarzane na obszarze Europejskiego Obszaru Gospodarczego.	
20	System musi na podstawie zebranych danych generować detekcje, stanowiące powiązane ze sobą podejrzane zdarzenia zarejestrowane na stacjach roboczych i serwerach.	
21	Detekcje muszą być generowane z wykorzystaniem statycznych reguł przygotowanych przez producenta oraz mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego Zamawiającego.	
22	Detekcje muszą być generowane w czasie rzeczywistym na podstawie danych przesyłanych przez agentów.	
23	Detekcje muszą być prezentowane w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie oraz powiązania pomiędzy elementami biorącymi udział w detekcji.	
24	System musi umożliwiać filtrowanie zdarzeń biorących udział w detekcji według poziomu ryzyka – od poziomu informacyjnego do krytycznego.	
25	Każda detekcja musi zawierać co najmniej: - listę urządzeń, na których zarejestrowano podejrzane zdarzenia, - datę i czas wystąpienia podejrzanych zdarzeń, - listę zidentyfikowanych podejrzanych zdarzeń, - opis każdego zdarzenia wyjaśniający, dlaczego zostało uznane za podejrzane, - sumę kontrolną (co najmniej SHA-1) plików uznanych za podejrzane, - poziom ryzyka określający istotność detekcji, - typ detekcji określający wykryte techniki ataku (np. nieuprawnione podniesienie uprawnień, połączenia z serwerami C&C, nieuprawnione wykonanie skryptu).	
26	Zdarzenia wskazujące na wykorzystanie znanej techniki ataku muszą zawierać odnośniki do ogólnodostępnych materiałów opisujących te techniki (np. matryca MITRE ATT&CK).	
27	Zdarzenia dotyczące plików i aplikacji uruchomionych na monitorowanych komputerach muszą zawierać odnośniki do ogólnodostępnej bazy reputacji plików (np. VirusTotal).	
28	System musi umożliwiać oznaczanie wygenerowanych detekcji jako fałszywie pozytywne. Oznaczenie musi powodować automatyczne identyfikowanie i odpowiednie oznaczanie przyszłych takich samych detekcji w konsoli zarządzającej.	
29	System musi umożliwiać utworzenie archiwum zawierającego dodatkowe informacje o hoście, na którym wystąpiła detekcja, na potrzeby analizy śledczej incydentu.	
30	System musi umożliwiać dodanie własnego komentarza do detekcji.	

31	System musi umożliwiać wykupienie usługi przesłania detekcji do analizy przez zespół ekspertów producenta, po której administrator otrzymuje szczegółowy raport dotyczący incydentu.	
32	System musi umożliwiać wysyłanie powiadomień e-mail o wygenerowaniu nowej detekcji.	
33	System musi umożliwiać ręczną izolację sieciową wybranych urządzeń przez administratora.	
34	System musi umożliwiać tworzenie reguł automatycznej izolacji sieciowej stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.	
35	System musi umożliwiać zdalne wykonywanie działań reakcji na chronionym hoście, w tym co najmniej: - pobranie plików, - pobranie historii PowerShell, - pobranie wpisów dziennika zdarzeń, - pobranie dziennika ochrony antywirusowej, - pobranie informacji o wpisach rejestru systemowego, - pobranie informacji o MBR, - wylistowanie procesów, usług oraz zadań harmonogramu zadań, - zatrzymanie procesu lub wątku, - usunięcie plików, usług, wartości rejestru systemowego oraz zadań harmonogramu zadań.	
36	System musi umożliwiać tworzenie raportów.	
37	System musi udostępniać dane o detekcjach za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami bezpieczeństwa, w tym z systemami klasy SIEM.	
38	Konsola zarządzająca musi posiadać panel kontrolny (dashboard) umożliwiający weryfikację stanu bezpieczeństwa organizacji.	
39	System musi umożliwiać wyszukiwanie zdarzeń napływających do konsoli co najmniej według: - PID oraz SHA-1 nowego procesu, - nazwy i ścieżki procesu, - nazwy i ścieżki procesu docelowego, - typu zdarzenia, - nazwy, typu i wersji systemu, - źródłowego i zdalnego adresu IP, - portu lokalnego i zdalnego, - wartości klucza rejestru.	
40	Konsola zarządzająca musi posiadać dedykowaną zakładkę z listą urządzeń z zainstalowanym agentem, zawierającą co najmniej: nazwę hosta, adres IP, poziom ważności, przypisany profil, system operacyjny, informację o ostatnim połączeniu oraz aktualny status.	
41	Administrator musi mieć możliwość tworzenia i usuwania kont administratorów w konsoli oraz nadawania im uprawnień.	
42	Konsola zarządzająca musi prezentować informacje o posiadanych licencjach, w tym: produkt, klucz licencyjny, typ licencji, wykorzystanie oraz datę wygaśnięcia.	
43	Konsola zarządzająca musi umożliwiać dodawanie kluczy licencyjnych innych produktów producenta, co najmniej systemu EPP oraz mechanizmu zarządzania ekspozycją na atak. Dodanie klucza musi skutkować aktywowaniem odpowiedniej funkcjonalności w konsoli.	
44	System musi posiadać wbudowane narzędzie, wykorzystujące mechanizmy	

	sztucznej inteligencji, do tworzenia podsumowania incydentu na podstawie dostępnych danych. Podsumowanie musi być generowane w języku konsoli zarządzającej.	
45	System musi umożliwiać wykupienie dodatkowych usług monitorowania oraz monitorowania i reagowania na incydenty (MDR), realizowanych przez zespoły bezpieczeństwa producenta. Wykupienie usługi nie może ograniczać administratorowi dostępu do konsoli ani wymagać reinstalacji agentów.	
46	Wykonawca dostarczy minimum licencję roczną (subskrypcję) systemu EDR dla co najmniej 7 urządzeń (stacji roboczych lub serwerów) wraz z prawem do aktualizacji, poprawek oraz wsparcia technicznego.	
47	Usługi wdrożenia: - Utworzenie i konfiguracja konta organizacji Zamawiającego w konsoli zarządzającej systemu EDR. - Konfiguracja kont i uprawnień administratorów konsoli. - Instalacja i konfiguracja agentów systemu EDR na 7 urządzeniach, w tym z wykorzystaniem mechanizmów dystrybucji Active Directory. - Weryfikacja poprawności działania zainstalowanych agentów.	

4. Oprogramowanie typu NDR – 1 szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Dostawa i instalacja oprogramowania klasy NDR, np. typu open source, w środowisku serwerowym Zamawiającego.	
2	Konfiguracja interfejsów zarządzających oraz interfejsów monitorujących systemu.	
3	Konfiguracja adresacji IP, DNS oraz synchronizacji czasu NTP.	
4	Konfiguracja dostępu administracyjnego do konsoli zarządzającej systemu.	
5	Integracja systemu z usługą katalogową Microsoft Active Directory lub LDAP.	
6	Konfiguracja ról, uprawnień oraz grup użytkowników administracyjnych.	
7	Konfiguracja źródeł ruchu sieciowego, w tym portów SPAN/mirror, TAP lub innych źródeł wskazanych przez Zamawiającego.	
8	Konfiguracja pasywnej analizy ruchu sieciowego oraz identyfikacji hostów, protokołów, sesji i połączeń.	
9	Konfiguracja mechanizmów detekcji zagrożeń, alertów bezpieczeństwa oraz reguł IDS, jeżeli dostępne	
10	Konfiguracja dashboardów, widoków analitycznych oraz podstawowych raportów.	

5. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IoT

Lp.	Parametry techniczne - wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Przygotowanie projektu wdrożenia rozwiązania z zakresu bezpieczeństwa biorąc pod uwagę dostarczone urządzania, oprogramowanie oraz usługi w zakresie obszaru IT	

6. NGFW (Next Gen FireWall) – 2 szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Wymagania ogólne System bezpieczeństwa musi być dostarczony w postaci dedykowanego urządzenia sprzętowego. System musi realizować funkcje sieciowe i bezpieczeństwa niezależnie od operatora i rodzaju wykorzystywanego łącza. System musi umożliwiać pracę co najmniej w trybach: • routera z funkcją NAT, • transparentnym, • monitorowania ruchu przekazywanego z portu SPAN lub TAP. System musi obsługiwać protokoły IPv4 oraz IPv6 w zakresie zapory sieciowej, routingu, połączeń VPN i mechanizmów ochronnych. System musi umożliwiać utworzenie minimum dwóch odseparowanych instancji logicznych obejmujących co najmniej routing, firewall, IPsec VPN, IPS, ochronę antywirusową i kontrolę aplikacji. System musi umożliwiać definiowanie kont administracyjnych i przydzielanie im uprawnień do poszczególnych instancji lub części konfiguracji.	
2	Redundancja i monitorowanie System musi umożliwiać łączenie dwóch urządzeń w klaster wysokiej dostępności pracujący w trybie Active-Passive lub Active-Active. Klaster musi umożliwiać synchronizację konfiguracji i aktywnych sesji firewall. System musi monitorować stan urządzenia, interfejsów, połączeń sieciowych oraz tuneli VPN. System musi umożliwiać agregację interfejsów statycznie oraz z wykorzystaniem protokołu LACP. System musi umożliwiać tworzenie interfejsów redundantnych. W przypadku dostarczenia klastra wszystkie urządzenia muszą być objęte jednakowym zakresem licencji i wsparcia producenta.	
3	Interfejsy i zasilanie Urządzenie musi posiadać co najmniej: • 5 portów 10/100/1000Base-T RJ45, • port konsolowy umożliwiający lokalne zarządzanie, • port USB. Wszystkie wymagane porty sieciowe muszą umożliwiać równoczesną pracę. System musi pozwalać na skonfigurowanie minimum 200 interfejsów wirtualnych VLAN zgodnych z IEEE 802.1Q. Urządzenie musi być wyposażone w zasilanie AC wraz z zasilaczem i przewodem umożliwiającym podłączenie do instalacji Zamawiającego.	
4	Parametry wydajnościowe System musi zapewniać co najmniej: • obsługę 700 000 jednoczesnych sesji firewall, • obsługę 83 000 nowych sesji na sekundę, • przepustowość Stateful Firewall dla pakietów 512 B - 5 Gbps, • przepustowość kontroli aplikacji - 2,8 Gbps,	

	• przepustowość IPsec VPN dla pakietów 512 B - 4,5 Gbps, • przepustowość IPS dla ruchu Enterprise Traffic Mix - 2,2 Gbps, • przepustowość NGFW dla ruchu Enterprise Traffic Mix, z włączonymi funkcjami Firewall, IPS i kontroli aplikacji - 1,2 Gbps, • przepustowość ochrony przed zagrożeniami dla ruchu Enterprise Traffic Mix, z włączonymi funkcjami Firewall, IPS, kontroli aplikacji i ochrony przed malware - 1,1 Gbps, • przepustowość inspekcji komunikacji SSL/TLS - 1,3 Gbps. Wartości muszą być potwierdzone w publicznie dostępnej dokumentacji producenta.	
5	Podstawowe funkcje bezpieczeństwa System musi realizować co najmniej: • zaporę sieciową klasy Stateful Inspection, • kontrolę aplikacji, • szyfrowane połączenia IPsec VPN, • ochronę antywirusową i przed malware, • ochronę IPS, • filtrowanie stron WWW, • ochronę przed komunikacją z sieciami botnet i serwerami C&C, • kontrolę zawartości poczty i ochronę antyspamową, • zarządzanie pasmem, QoS i Traffic Shaping, • inspekcję ruchu szyfrowanego SSL/TLS, • uwierzytelnianie wieloskładnikowe z wykorzystaniem tokenów sprzętowych lub programowych, • automatyczne wykonywanie zdefiniowanych akcji po wystąpieniu określonego zdarzenia bezpieczeństwa.	
6	Polityki firewall i NAT Polityki firewall muszą umożliwiać uwzględnienie co najmniej: • źródłowych i docelowych adresów IP, • użytkowników i grup użytkowników, • interfejsów oraz stref bezpieczeństwa, • protokołów i usług, • aplikacji lub kategorii aplikacji, • harmonogramów, • profili bezpieczeństwa, • rejestrowania zdarzeń. System musi obsługiwać: • źródłową i docelową translację adresów, • PAT, • translację jeden do jednego oraz jeden do wielu, • dedykowany ALG dla protokołu SIP. System musi umożliwiać tworzenie stref bezpieczeństwa, np. LAN, WAN i DMZ. System musi umożliwiać filtrowanie ruchu na podstawie kraju przypisanego do źródłowego lub docelowego adresu IP. System musi umożliwiać korzystanie z zewnętrznych źródeł zawierających adresy IP, domeny lub adresy URL. System musi pozwalać na określenie czasu aktywności poszczególnych reguł firewall.	
7	System musi obsługiwać co najmniej: • IKEv1 oraz IKEv2,	

	• szyfrowanie AES-128 i AES-256, w tym tryb GCM, • grupy Diffie-Hellman co najmniej 19 i 20, • tunele Site-to-Site oraz Client-to-Site, • topologie Hub-and-Spoke oraz Mesh, • uwierzytelnianie kluczem współdzielonym i certyfikatem, • routing statyczny i dynamiczny przez tunele VPN, • IPsec NAT Traversal, DPD i XAuth, • mechanizm Split Tunneling, • monitorowanie dostępności tuneli i automatyczne uruchamianie tunelu zapasowego, • ograniczanie liczby jednocześnie negocjowanych tuneli w celu ochrony zasobów systemu. Producent musi posiadać w ofercie oprogramowanie klienckie umożliwiające zestawianie połączeń VPN.	
8	Routing, SD-WAN i zarządzanie pasmem System musi obsługiwać: • routing statyczny, • Policy Based Routing, • RIPv2 i RIPng, • OSPF i OSPFv3, • BGP, • PIM, • filtrowanie tras, • ECMP, • BFD. System musi monitorować dostępność wskazanego adresu IP i automatycznie modyfikować tablicę routingu po wykryciu awarii. Mechanizm SD-WAN musi obsługiwać interfejsy fizyczne i wirtualne, w tym VLAN oraz IPsec. System musi umożliwiać wybór łącza na podstawie parametrów jakościowych, dostępności oraz zdefiniowanych reguł. Zarządzanie pasmem musi umożliwiać: • określenie pasma maksymalnego i gwarantowanego, • określenie priorytetu ruchu, • oznaczanie DSCP, definiowanie limitów dla aplikacji, użytkowników i kategorii URL.	
9	Ochrona przed malware • System musi skanować ruch w obu kierunkach, również dla aplikacji pracujących na niestandardowych portach. • Skanowanie musi obejmować co najmniej HTTP, HTTPS, FTP, POP3, IMAP, SMTP i CIFS. • System musi umożliwiać analizowanie archiwów ZIP i RAR, w tym archiwów zagnieżdżonych. • System musi umożliwiać blokowanie archiwów zaszyfrowanych, uszkodzonych lub niemożliwych do przeskanowania. • System musi posiadać sygnatury malware dla urządzeń mobilnych, co najmniej dla systemu Android. • Bazy sygnatur muszą być aktualizowane automatycznie. • System musi umożliwiać przesyłanie plików do chmurowej usługi Sandbox w celu wykrywania nieznanych zagrożeń oraz wykorzystywanie informacji	

	o złośliwych adresach URL do blokowania niebezpiecznej komunikacji. • System musi wykorzystywać mechanizmy heurystyczne i uczenie maszynowe do wykrywania zagrożeń. Administrator musi mieć możliwość zastosowania ochrony antywirusowej wyłącznie dla wybranych polityk i zakresów ruchu.	
10	Ochrona IPS i kontrola aplikacji • Ochrona IPS musi wykorzystywać analizę sygnaturową oraz analizę anomalii protokołów. • System musi chronić aplikacje działające na standardowych i niestandardowych portach. • Baza IPS musi zawierać minimum 5000 sygnatur i być aktualizowana automatycznie. • Administrator musi mieć możliwość definiowania własnych sygnatur i wyjątków. • System musi wykrywać anomalie ruchu oraz zapewniać ochronę przed atakami DoS i DDoS. • System musi wykrywać i blokować komunikację z sieciami botnet i serwerami C&C. • Funkcje IPS muszą być przypisywane do wybranych polityk firewall. • Kontrola aplikacji musi wykorzystywać głęboką analizę pakietów i nie może bazować wyłącznie na numerach portów TCP/UDP. • Baza kontroli aplikacji musi zawierać minimum 2000 sygnatur. • System musi umożliwiać kontrolowanie operacji wykonywanych w aplikacjach chmurowych, w tym przesyłania i pobierania plików. System musi umożliwiać blokowanie aplikacji typu proxy i P2P oraz aplikacji wykorzystujących niestandardowe porty.	
11	Moduł filtrowania WWW musi wykorzystywać aktualizowaną przez producenta bazę adresów URL pogrupowanych w kategorie. Dostępne kategorie muszą obejmować co najmniej malware, phishing, spam, proxy, Dynamic DNS i treści zabronione prawem. Administrator musi mieć możliwość: • nadpisywania kategorii, • tworzenia białych i czarnych list, • definiowania adresów z wykorzystaniem wyrażeń regularnych, • wyświetlania użytkownikowi ostrzeżenia wymagającego potwierdzenia, • definiowania własnych komunikatów blokady, • wyłączania wskazanych kategorii lub adresów URL z inspekcji SSL/TLS. System musi obsługiwać mechanizm Safe Search. Ochrona poczty musi wykorzystywać bazy reputacyjne adresów IP, domen, nadawców i sum kontrolnych wiadomości.	
12	Uwierzytelnianie użytkowników System musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: • lokalnej bazy użytkowników, • LDAP i Microsoft Active Directory, • RADIUS, • zewnętrznych systemów uwierzytelniania, • protokołu SAML. System musi umożliwiać integrację z Active Directory w celu realizacji Single Sign-On.	

	Tożsamość użytkownika lub grupy musi być możliwa do wykorzystania bezpośrednio w politykach firewall. System musi umożliwiać stosowanie uwierzytelniania dwuskładnikowego dla administratorów oraz użytkowników połączeń VPN.	
13	Uwierzytelnianie użytkowników System musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: • lokalnej bazy użytkowników, • LDAP i Microsoft Active Directory, • RADIUS, • zewnętrznych systemów uwierzytelniania, • protokołu SAML. System musi umożliwiać integrację z Active Directory w celu realizacji Single Sign-On. Tożsamość użytkownika lub grupy musi być możliwa do wykorzystania bezpośrednio w politykach firewall. System musi umożliwiać stosowanie uwierzytelniania dwuskładnikowego dla administratorów oraz użytkowników połączeń VPN.	
14	Zarządzanie i diagnostyka System musi umożliwiać lokalne zarządzanie poprzez HTTPS i SSH. System musi umożliwiać współpracę z centralnymi platformami zarządzania i monitorowania producenta. System musi obsługiwać: • SNMPv2c i SNMPv3, • NetFlow lub sFlow, • API z publicznie dostępną dokumentacją. System musi posiadać narzędzia diagnostyczne obejmujące co najmniej ping, traceroute, przechwytywanie pakietów oraz diagnostykę sesji firewall. System musi umożliwiać: • uwierzytelnianie dwuskładnikowe administratorów, • tworzenie profili administracyjnych o różnych uprawnieniach, • ograniczenie dostępu administracyjnego do wskazanych adresów źródłowych, System musi umożliwiać współpracę z centralną platformą zarządzania producenta, pozwalającą na realizację zmian konfiguracyjnych w trybie workflow, z ich zatwierdzaniem przed zastosowaniem.	
15	Logowanie System musi rejestrować co najmniej: • ruch zaakceptowany i zablokowany, • aktywność administratorów, • zdarzenia modułów bezpieczeństwa, • wykorzystanie zasobów, • stan pracy urządzenia. System musi umożliwiać włączenie lub wyłączenie logowania dla każdej reguły firewall. System musi umożliwiać jednoczesne przekazywanie logów do wielu zewnętrznych systemów. System musi obsługiwać protokół SYSLOG, w tym transmisję przez TCP oraz komunikację szyfrowaną SSL/TLS.	
16	Licencje bezpieczeństwa IT i OT Dla urządzenia należy dostarczyć aktywne licencje bezpieczeństwa na okres minimum 12 miesięcy, obejmujące co najmniej:	

	• aktualizacje kontroli aplikacji, • aktualizacje IPS, • ochronę antywirusową i Advanced Malware Protection, • ochronę urządzeń mobilnych, • ochronę przed nowymi ogniskami zagrożeń, • analizę plików w chmurowej usłudze Sandbox, • ochronę przed botnetami i komunikacją C&C, • bazy reputacyjne adresów IP, domen i certyfikatów, • ochronę antyspamową; • usługę bezpieczeństwa OT, zapewniającą co najmniej: • wykrywanie urządzeń, aplikacji, usług i protokołów OT, • korelację podatności i wirtualne łatanie urządzeń OT, • sygnatury Application Control i IPS dla OT.	
17	Gwarancja i wsparcie producenta Urządzenie musi zostać objęte aktywnym wsparciem producenta przez okres minimum 12 miesięcy od dnia odbioru. Wsparcie musi obejmować co najmniej: • pomoc techniczną producenta w trybie 24×7×365, • czas reakcji dla zgłoszeń krytycznych nie dłuższy niż 1 godzina, • dostęp do aktualizacji oprogramowania systemowego, • dostęp do portalu wsparcia i narzędzi producenta, • możliwość zgłaszania problemów przez portal internetowy i telefonicznie, • zaawansowaną wymianę uszkodzonego urządzenia w trybie AHR, zgodnie z warunkami producenta. • Licencje i wsparcie muszą być widoczne na koncie Zamawiającego.	

7. Usługa konfiguracji i hardening systemów/urządzeń IT/OT/ICS/IIoT

Lp.	Parametry techniczne - wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Usługa konfiguracji i hardeningu dla dostarczanych urządzeń i oprogramowania zgodnie z najlepszymi praktykami i rekomendacjami producentów.	

8. Stacja robocza fizyczna lub wirtualna z rolą stacji przesiadkowej – 2 szt.

Lp.	Parametry techniczne - wymagania minimalne	
Parametry techniczne - wymagania minimalne		**Producent:** …… **Model:** …… **Spełnia wymogi Tak/Nie (wpisać poniżej)**
1	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta	
2	Obudowa: Małogabarytowa typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu, umożliwiająca montaż wewnątrz obudowy napędu optycznego w dedykowanej zewnętrznej wnęce 5.25” typu Slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Obudowa jednostki centralnej musi umożliwiać demontaż pokrywy w celu uzyskania dostępu do podzespołów. Dopuszcza się mocowanie pokrywy za pomocą śrub zabezpieczonych przed wypadnięciem. Moduł konstrukcji obudowy komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Suma wymiarów obudowy mierzona po krawędziach obudowy nie może przekraczać 700 mm.	
3	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logo producenta oferowanej jednostki dedykowana dla danego urządzenia wyposażona w sloty i złącza: 4 złącza DIMM z obsługą do 128 GB pamięci RAM DDR5, 3 złącza M.2 dedykowane dla dysku SSD, 1 złącze M.2 WLAN, 1 złącze PCIe x16 Gen 4.0, 1 złącze PCIe x4 Gen 3.0, 1 złącze PCIe x1 Gen 3.0, 2 złącza SATA 3.0.	
4	Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 34 000pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php.	
5	Zainstalowana pamięć RAM: minimum 16 GB DDR5, pracująca z prędkością minimum 4800 MT/s. Możliwość rozbudowy pamięci do minimum 128 GB. Komputer musi posiadać minimum cztery sloty pamięci, z których co najmniej dwa pozostają wolne w dostarczonej konfiguracji.	
6	Dysk SSD 512GB	
7	Zintegrowana karta graficzna	
8	Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), karta WiFi 6	
9	Karta dźwiękowa zintegrowana z płytą główną	
10	Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez	

	stosowania przejściówek, adapterów, rozgałęziaczy itp.: Panel przedni: 1 x Universal audio jack (słuchawki i mikrofon) 1 x USB 3.2 Gen 2 typu A 1 x USB 3.2 Gen 2x2 typu C 2 x USB 2.0 Panel tylny: 3 x DisplayPort 1.4a 1 x USB 3.2 Gen 2 typu C 3 x USB 3.2 Gen 1 typu A 2 x USB 2.0 1 x RJ45 10/100/1000	
11	Dedykowany układ sprzętowy TPM min. 2.0. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (wbudowane w obudowę gniazdo blokady Kensington) oraz kłódki (oczko w obudowie do założenia kłódki).	
12	Możliwość odczytania z BIOS informacji o: • Wersji BIOS • Numerze seryjnym komputera • Numerze inwentarzowym • Typie (modelu) procesora, ilości rdzeni. • Ilości pamieci RAM, jej prędkości oraz obsadzeniu w slotach. • Pojemności i modelu zainstalowanego dysku. • MAC adresie zintegrowanej karty sieciowej • Technologii zdalnego zarządzania (o ile występuje) BIOS musi umożliwiać: • Włączenie/wyłączenie zintegrowanej karty sieciowej • Włączenie/wyłączenie karty sieci bezprzewodowej oraz Bluetooth (o ile występuje) • Włączenie/wyłączenie karty audio • Włączenie/wyłączenie poszczególnych portów USB Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny.	
13	W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać: • Nadanie hasła administratora • Ustawienie hasła dla zainstalowanego dysku • Ustawienie portów USB wtrybie „No BOOT” • Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej • Zarządzanie funkcją Secure Boot • Zarządzanie układem TPM • Zarządzania funkcją tworzenia recovery BIOS • Zarządzania funkcją downgrade BIOS. • Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia. Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny.	

14	Komputer musi posiadać wbudowany w BIOS/UEFI system diagnostyczny sprzętu z graficznym interfejsem użytkownika, dostępny z menu rozruchowego i działający bez uruchamiania systemu operacyjnego. System musi umożliwiać obsługę z wykorzystaniem klawiatury oraz wykonywanie testów komponentów sprzętowych. Diagnostyka pozostałych komponentów musi być dostępna również przy braku, uszkodzeniu lub sformatowaniu dysku oraz bez dostępu do sieci i internetu. Uruchomienie diagnostyki nie może wymagać dodatkowych nośników ani instalowania oprogramowania na dysku komputera.	
15	Wbudowany wizualny system diagnostyczny usytuowany na przednim panelu obudowy, działający w oparciu sygnalizację LED wbudowaną np. w przycisk włącznika komputera. System służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami poprzez zmianę statusów wyświetlania diody (miganie w określonej sekwencji oraz zmiana barw wyświetlania). System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.	
16	Zasilacz o mocy min.360W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 80% przy obciążeniu zasilacza na poziomie 100%, Potwierdzeniem wymaganej sprawności może być dokumentacja producenta oferowanego modelu komputera wskazująca zastosowanie zasilacza o klasie sprawności 80 PLUS Platinium lub wyższej, albo raport z badań zasilacza potwierdzający wymagane wartości sprawności.	
17	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).	
18	Zainstalowany system operacyjny Windows 11 Pro, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego na podstawie dołączonego nośnika bez potrzeby ręcznego wpisywania klucza licencyjnego.	
19	Mysz i klawiatura.	
20	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, aktualizacje, diagnostyka, dedykowane oprogramowanie).	
21	Firma serwisująca musi posiadać ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami na	

	świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Gwaranacja na okres 3 lat	
22	Producent komputera musi udostępniać bezpłatne oprogramowanie z nieograniczoną czasowo licencją na użytkowanie, możliwe do pobrania i zainstalowania przez Zamawiającego, umożliwiające: - upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.	
Parametry monitora		**Producent:** **……** **Model:** **……** **Spełnia wymogi Tak/Nie (wpisać poniżej w pustych polach)**
1	Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą IPS o przekątnej min. 26.95"	

2	Rozmiar plamki (maksymalnie) 0,312 mm x 0,312 mm	
3	Jasność 300 cd/m2	
4	Kontrast statyczny 1500:1	
5	Kąty widzenia (pion/poziom) 178/178 stopni	
6	Czas reakcji matrycy (maksymalnie) 8ms (gray to gray)	
7	Rozdzielczość maksymalna 1920 x 1080 przy 120Hz (dotyczy cyfrowych portów wideo)	
8	Gama koloru sRGB 99%	
9	Pochylenie monitora W zakresie 26 stopni	
10	Wydłużenie w pionie Tak, min. 150 mm	
11	PIVOT −90° do +90° stopni	
12	Obrót lewo/prawo W zakresie min. (-45/+45) stopni	
13	Powłoka powierzchni ekranu Antyodblaskowa	
14	Podświetlanie System podświetlania LED	
15	Zużycie energii Całkowite zużycie energii (kWh/rok): maks. 45 kWh rocznie Dane zużycia do zweryfikowania na stronie Energy Star: https://www.energystar.gov/productfinder/	
16	Bezpieczeństwo Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą	
17	Złącza: 1 x HDMI 1.4 lub nowszy 1 x DisplayPort 1.2 lub nowszy 2 x USB 3.2 Gen 1 Typ A 1 x USB 3.2 Gen 1 typu C 1 x USB 3.2 Gen 1 typu B	
18	Czas trwania gwarancji min. 3 lata. Firma serwisująca musi posiadać ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. Oświadczenie producenta monitor, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
19	Certyfikaty Certyfikat ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie	

	ryzykiem oraz zgodność z przepisami dla producenta monitora (załączyć dokument potwierdzający spełnianie wymogu) Certyfikat ISO 14001 lub równoważny spełniający wymagania związane z zarządzaniem środowiskowym, zgodnością z przepisami, ciągłym doskonaleniem na rzecz ochrony środowiska, monitorowaniem wpływu na środowisko dla producenta monitora (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE	
20	Oprogramowanie Dołączone oprogramowanie producenta monitora z bezterminową licencją na użytkowanie, umożliwiające zarządzanie oferowanym monitorem bezpośrednio z poziomu systemu operacyjnego podłączonego komputera w zakresie: • Konfiguracji ustawień wyświetlania obrazu, w tym min: o jasność i kontrast (w trybie ręcznym oraz według ustalonego przez użytkownika harmonogramu), o kolor (w trybie ręcznym oraz automatycznym dla określonych aplikacji), o rozdzielczość wyświetlania, częstotliwość odświeżania ekranu oraz orientacja ekranu. • Sposobu wyświetlania wielu okien poszczególnych aplikacji jednocześnie w predefiniowanym lub niestandardowym (stworzonym przez użytkownika) układzie, z możliwością przypisania układu wyświetlania okien do konkretnych aplikacji. • Aktualizacji oprogramowania układowego monitora oraz oprogramowania zarządzającego. • Możliwość wyeksportowania oraz importowania ustawień.	

9. Usługa segmentacji sieci IT/OT/ICS/IIoT

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Przeprowadzenie analizy obecnej architektury sieciowej Zamawiającego w zakresie obszarów IT oraz OT/ICS/IIoT, obejmującej identyfikację głównych segmentów, podsieci, VLAN, urządzeń, systemów oraz przepływów komunikacyjnych.	
2	Opracowanie koncepcji logicznej segmentacji sieci z podziałem na obszary funkcjonalne, w tym co najmniej sieć użytkowników, serwerów, zarządzania, urządzeń bezpieczeństwa, systemów OT/ICS/IIoT oraz stref pośrednich/DMZ, jeżeli są wymagane.	
3	Opracowanie zasad separacji komunikacji pomiędzy segmentami sieci, w szczególności pomiędzy obszarem IT i OT/ICS/IIoT, z uwzględnieniem zasady minimalnego wymaganego dostępu.	
4	Konfiguracja segmentów logicznych sieci, w tym VLAN, podsieci IP, interfejsów logicznych, trasowania oraz innych mechanizmów separacji dostępnych w infrastrukturze Zamawiającego, jeżeli są wymagane.	
5	Konfiguracja polityk kontroli ruchu pomiędzy segmentami sieci, obejmujących dopuszczenie wyłącznie wymaganych kierunków komunikacji, adresów źródłowych i docelowych, portów, protokołów oraz usług.	
6	Konfiguracja segmentacji dla obszaru OT/ICS/IIoT w sposób ograniczający bezpośrednią komunikację pomiędzy systemami przemysłowymi a siecią IT oraz Internetem, z uwzględnieniem wymagań ciągłości działania środowiska przemysłowego.	
7	Konfiguracja strefy pośredniej/DMZ lub innego mechanizmu kontrolowanej wymiany danych pomiędzy obszarem IT i OT/ICS/IIoT, jeżeli jest wymagany przez architekturę Zamawiającego.	
8	Konfiguracja dostępu administracyjnego do wybranych segmentów sieci, w tym ograniczenie dostępu zarządczego wyłącznie do wskazanych użytkowników, stacji administracyjnych, adresów IP lub systemów zarządzających.	
9	Konfiguracja podstawowych mechanizmów monitorowania i logowania ruchu pomiędzy segmentami sieci, w szczególności dla komunikacji pomiędzy obszarem IT i OT/ICS/IIoT oraz dla ruchu blokowanego przez polityki bezpieczeństwa.	
10	Przeprowadzenie testów funkcjonalnych wdrożonej segmentacji, obejmujących weryfikację dostępności wymaganych usług, blokowanie komunikacji niedozwolonej oraz poprawność działania reguł separacji pomiędzy segmentami.	
11	Wprowadzenie uzgodnionych korekt konfiguracyjnych wynikających z przeprowadzonych testów, z zachowaniem wymagań bezpieczeństwa oraz ciągłości działania systemów Zamawiającego.	
12	Przekazanie Zamawiającemu dokumentacji powykonawczej obejmującej opis segmentów sieci, adresację IP, VLAN, skonfigurowane polityki bezpieczeństwa.	

10. Network Attached Storage (NAS) – 2 szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Obudowa typu Rack o wysokości maksymalnie 2U w konfiguracji umożliwiającej instalację minimum 12 dysków w formice 3,5”. Urządzenie musi umożliwiać wymianę dysków podczas pracy (Hot-Swap).	
2	Procesor: Zainstalowany min. 1 procesor klasy x86 min. 4-rdzeniowy o taktowaniu min. 2.4GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 5 000 pkt. Testy dla oferowanego modelu procesora muszą być opublikowane i ogólnie dostępne na stronie: https://www.cpubenchmark.net/cpu_list.php	
3	Pamięć RAM – minimum 8GB DDR4 wraz z obsługą korekcji błędów ECC.	
4	Przestrzeń dyskowa: Zainstalowane: - minimum 12 dysków o pojemności min. 4TB	
5	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 1Gbps RJ45	
6	Porty i gniazda PCIe - Minimum 2 porty USB 3.0 lub USB 3.2 Gen 1, - Minimum 2 porty rozszerzeń umożliwiające podłączenie zewnętrznych jednostek rozszerzających przestrzeń dyskową, - Minimum 2 gniazda PCIe Gen3 x8, - Możliwość rozbudowy urządzenia do minimum 36 zatok dyskowych z wykorzystaniem kompatybilnych jednostek rozszerzających.	
7	Funkcjonalność kontrolera dyskowego: - Obsługa RAID 0,1,5,6,10, - Obsługa Hot Spare, - Obsługa JBOD,	
8	Szyfrowanie: - Musi umożliwiać szyfrowanie wybranych udziałów sieciowych, kluczem co najmniej AES-256 bitów.	
9	Obsługiwane protokoły: - SMB/CIFS, - AFP, - NFS, - FTP, - WebDAV, - iSCSI, - SSH, - SNMP, - HTTP/HTTPS, - Rsync.	
10	Funkcjonalności: - Serwer VPN,	

	- Serwer WWW, - Serwer plików, - Menedżer plików dostępny przez WWW, - Zdalna replikacja lub synchronizacja danych z szyfrowaniem transmisji, - Obsługa wielu zadań synchronizacji lub backupu do różnych serwerów, - Obsługa DDNS, - Monitorowanie stanu dysków (S.M.A.R.T.), - Diagnostyka dysków i wykrywanie uszkodzonych sektorów, - Monitorowanie systemu i powiadomienia o awariach, - Zarządzanie urządzeniem przez interfejs WWW.	
11	Obsługa wolumenów: - Obsługa minimum 128 wolumenów - Obsługa minimum 64 Targetów iSCSI - Obsługa minimum 128 lunów - Obsługa minimum 100 kont użytkowników - Obsługa minimum 50 grup użytkowników	
12	Zasilanie Zasilacz o mocy co najmniej 500W	
13	Gwarancja 36 miesięcy gwarancji producenta na serwer NAS oraz dyski	

11. System operacyjny i/lub licencje dostępowe (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 1 komplet

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi |Tak/Nie (wpisać poniżej)
1	Oprogramowanie systemu operacyjnego Microsoft Windows Server 2025 Standard 16 Core - 1szt Microsoft Windows Server 2025 User CAL – 10szt Licencja wieczysta umożliwiająca legalne użytkowanie oprogramowania systemu operacyjnego na oferowanym serwerze. Opis równoważności znajduje się pod tabelą. Zamawiający dopuszcza rozwiązanie OEM	

OPIS RÓWNOWAŻNOŚCI

1) Współpraca z procesorami o architekturze x86-64.
2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3) Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.
4) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2019.
5) Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
6) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
10) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
11) Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
12) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
13) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
14) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

–Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

–Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,

–Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.

–Zdalna dystrybucja oprogramowania na stacje robocze.

–Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

–PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

- Dystrybucję certyfikatów poprzez http,
- Konsolidację CA dla wielu lasów domeny,
- Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.

–Szyfrowanie plików i folderów.

–Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

–Serwis udostępniania stron WWW.

–Wsparcie dla protokołu IP w wersji 6 (IPv6).

–Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

17) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

18) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

19) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.

12. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 1szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Obudowa typu Rack o wysokości maksymalnie 1U w konfiguracji pozwalającej zainstalować 8 dysków twardych. Komplet wysuwanych szyn i organizer okablowania, umożliwiający montaż w szafie rack i wysuwanie do celów serwisowych.	
2	Płyta główna – pozwalająca na zainstalowanie jednego procesora zaprojektowana przez producenta węzła i oznaczona jego znakiem firmowym.	
3	Chipset - dedykowany przez producenta procesora do pracy w systemach jednoprocesorowych.	
4	Procesory - zainstalowane jeden procesor minimum 16-rdzeniowy klasy x86 uzyskujące w teście „SPECrate2017_fp_base" dostępnym na stronie www.spec.org dla konfiguracji z jednym procesorem wyniku min. 298 punktów. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego procesora w oferowanym modelu serwera. Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie zastosowanego w projekcie oprogramowania.	
5	Pamięć RAM – minimum 128 GB DDR5 RDIMM 5600MT/s. Płyta główna powinna obsługiwać do minimum 1TB pamięci RAM dla konfiguracji jednoprocesorowej. Pojemność zastosowanych kości pamięci RAM min. 64 GB.	
6	Zabezpieczenia pamięci RAM - ECC	
7	Gniazda PCI – minimum dwa sloty PCIe	
8	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 1Gbps Base-T - minimum 2 porty typu Ethernet 10/25Gbps SFP28	
9	Przestrzeń dyskowa: - dysk twardy typu HDD o pojemności minimum 1,2TB, każdy – 8szt, skonfigurowane w RAID5.	
10	Wbudowane porty: - minimum 1 port USB 2.0 - minimum 2 porty USB 3.0, - 1 port RJ45 dedykowany do zarządzania, - 1 porty VGA	
11	Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	
12	Wentylatory - redundantne	
13	Zasilacze - redundantne, Hot-Plug minimum 800W.	
14	Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność: - komunikacja poprzez interfejs RJ45, - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,	

	- wbudowana diagnostyka, - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym, - lokalna oraz zdalna konfiguracja serwera, - wsparcie dla IPv4 i IPv6, - obsługa komunikacji szyfrowanej tls 1.2 oraz tls 1.3 - możliwość zdalnego dostępu do konsoli graficznej z przejęciem kontroli nad klawiaturą i myszką, zainstalowanego systemu operacyjnego serwera.	
15	Urządzenie musi być wyprodukowane zgodnie z normą ISO-9001:2015 oraz ISO-14001. Urządzenie musi być zgodne z normami UE i przeznaczone na rynek UE, musi posiadać certyfikat CE.	
16	Dostarczone urządzenia muszą być fabrycznie nowe, nieregenerowane i wyprodukowane najwcześniej w ciągu ostatnich 6 miesięcy przed dostawą, muszą pochodzić z oficjalnego kanału sprzedaży producenta na teren Polski	
17	Oferowane urządzenie musi być objęte co najmniej 3-letnim wsparciem producenta sprzętu w dni robocze, czas reakcji w miejscu instalacji sprzętu Następny Dzień Roboczy. Musi istnieć możliwość sprawdzenia na stronie WWW producenta serwera, prowadzonej w języku polskim, po podaniu numeru seryjnego urządzenia minimum: - okresu oraz poziomu gwarancji, - zainstalowanych komponentów (w tym m.in. procesorów, pamięci RAM, dysków, zasilaczy i kart komunikacyjnych). Adres strony WWW producenta na której można sprawdzić powyższe dane musi być podany w złożonej ofercie.	
18	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.	

13. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 1szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Obudowa typu Rack o wysokości maksymalnie 1U w konfiguracji pozwalającej zainstalować 8 dysków twardych. Komplet wysuwanych szyn i organizer okablowania, umożliwiający montaż w szafie rack i wysuwanie do celów serwisowych.	
2	Płyta główna – pozwalająca na zainstalowanie jednego procesora zaprojektowana przez producenta węzła i oznaczona jego znakiem firmowym.	
3	Chipset - dedykowany przez producenta procesora do pracy w systemach jednoprocesorowych.	
4	Procesory - zainstalowane jeden procesor minimum 16-rdzeniowy klasy x86 uzyskujące w teście „SPECrate2017_fp_base" dostępnym na stronie www.spec.org dla konfiguracji z jednym procesorem wyniku min. 298 punktów. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego procesora w oferowanym modelu serwera. Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie zastosowanego w projekcie oprogramowania.	
5	Pamięć RAM – minimum 128 GB DDR5 RDIMM 5600MT/s. Płyta główna powinna obsługiwać do minimum 1TB pamięci RAM dla konfiguracji jednoprocesorowej. Pojemność zastosowanych kości pamięci RAM min. 64 GB.	
6	Zabezpieczenia pamięci RAM - ECC	
7	Gniazda PCI – minimum dwa sloty PCIe	
8	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 1Gbps Base-T - minimum 2 porty typu Ethernet 10/25Gbps SFP28	
9	Przestrzeń dyskowa: - dysk twardy typu HDD o pojemności minimum 1,2TB, każdy – 8szt, skonfigurowane w RAID5.	
10	Wbudowane porty: - minimum 1 port USB 2.0 - minimum 2 porty USB 3.0, - 1 port RJ45 dedykowany do zarządzania, - 1 porty VGA	
11	Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	
12	Wentylatory - redundantne	
13	Zasilacze - redundantne, Hot-Plug minimum 800W.	
14	Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność: - komunikacja poprzez interfejs RJ45, - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,	

	- wbudowana diagnostyka, - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym, - lokalna oraz zdalna konfiguracja serwera, - wsparcie dla IPv4 i IPv6, - obsługa komunikacji szyfrowanej tls 1.2 oraz tls 1.3 - możliwość zdalnego dostępu do konsoli graficznej z przejęciem kontroli nad klawiaturą i myszką, zainstalowanego systemu operacyjnego serwera.	
15	Urządzenie musi być wyprodukowane zgodnie z normą ISO-9001:2015 oraz ISO-14001. Urządzenie musi być zgodne z normami UE i przeznaczone na rynek UE, musi posiadać certyfikat CE.	
16	Dostarczone urządzenia muszą być fabrycznie nowe, nieregenerowane i wyprodukowane najwcześniej w ciągu ostatnich 6 miesięcy przed dostawą, muszą pochodzić z oficjalnego kanału sprzedaży producenta na teren Polski	
17	Oferowane urządzenie musi być objęte co najmniej 3-letnim wsparciem producenta sprzętu w dni robocze, czas reakcji w miejscu instalacji sprzętu Następny Dzień Roboczy. Musi istnieć możliwość sprawdzenia na stronie WWW producenta serwera, prowadzonej w języku polskim, po podaniu numeru seryjnego urządzenia minimum: - okresu oraz poziomu gwarancji, - zainstalowanych komponentów (w tym m.in. procesorów, pamięci RAM, dysków, zasilaczy i kart komunikacyjnych). Adres strony WWW producenta na której można sprawdzić powyższe dane musi być podany w złożonej ofercie.	
18	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.	

14. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Wysokość 27U	
2	Wymiary 800x1000 mm	
3	Szafa RACK do samodzielnego montażu – Zamawiający wymaga zamontowania szafy przez Wykonawcę	
4	Kolor: RAL 9004	
5	Obciążenie: min 790 kg	
6	Drzwi: przednie perforowane (stalowe, jednoskrzydłowe) zamykane na zamek tylne perforowane (stalowe) zamykane na zamek	
7	Ściany pełne stalowe, zdejmowane na zatrzaskach, zamykane na klucz	
8	Przepusty kablowe: górny oraz dolny	
9	Wymagane jest dostarczenie panelu LCD z termostatem i wbudowanym sufitowym panelem wyposażonym w min. 4 wentylatory	
10	Gwarancja 24miesiące	

15. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X(Switch) – 1 komplet

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Typ Obudowy: Przełącznik zarządzalny, przeznaczony do montażu w szafie RACK 19”, o wysokości maksymalnie 1U. Urządzenie musi zostać dostarczone wraz z kompletem elementów wymaganych do montażu w szafie RACK.	
2	Porty: Urządzenie musi posiadać co najmniej • 24 porty 10/100/1000Base-T RJ45, • 4 porty 1/10 Gigabit Ethernet SFP+, • 1 port konsolowy RJ45 umożliwiający lokalne zarządzanie urządzeniem.	
3	Wydajność: • Przepustowość przełącznika minimum 128Gbps, • Wydajność przełączania minimum 190Mpps, • Obsługa minimum 32,000 adresów MAC, • Bufor pakietów o pojemności minimum 2MB, • Obsługę minimum 4000 VLAN.	
4	Zasilanie: Wbudowany zasilacz przystosowany do zasilania napięciem 100–240 V AC, 50/60 Hz. Urządzenie musi zostać dostarczone z przewodem zasilającym umożliwiającym podłączenie do instalacji Zamawiającego.	
5	Funkcje sieciowe: Urządzenie musi obsługiwać co najmniej: • sieci VLAN zgodne z IEEE 802.1Q, • IEEE 802.1D – STP, • IEEE 802.1w – RSTP, • IEEE 802.1s – MSTP, • agregację łączy z wykorzystaniem LACP, • LLDP oraz LLDP-MED, • IGMP Snooping, • Port Mirroring, • mechanizmy ochrony STP, w tym BPDU Guard, Root Guard lub Loop Guard, • kontrolę ruchu broadcast, multicast i unknown unicast - Storm Control, • mechanizmy QoS, obejmujące klasyfikowanie, oznaczanie i kolejkowanie ruchu, • routing statyczny dla protokołów IPv4 oraz IPv6, • funkcję DHCP Relay.	
6	Bezpieczeństwo i kontrola dostępu Urządzenie musi obsługiwać co najmniej: • uwierzytelnianie użytkowników i urządzeń zgodne z IEEE 802.1X, • uwierzytelnianie urządzeń na podstawie adresu MAC – MAB, • dynamiczne przypisywanie użytkowników lub urządzeń do sieci VLAN na podstawie informacji otrzymanych z serwera RADIUS,	

	• uwierzytelnianie administratorów z wykorzystaniem RADIUS oraz TACACS+, • listy kontroli dostępu ACL dla ruchu IPv4, • DHCP Snooping, • ograniczanie liczby adresów MAC obsługiwanych na porcie, • mechanizmy ochrony przed nieautoryzowanym podłączeniem urządzeń do portów przełącznika.	
7	Zarządzanie i monitorowanie Urządzenie musi zapewniać: • zarządzanie poprzez graficzny interfejs użytkownika dostępny przez HTTPS, • zarządzanie poprzez interfejs CLI z wykorzystaniem SSHv2, • lokalny dostęp administracyjny przez port konsolowy, • obsługę SNMPv2c oraz SNMPv3, • przesyłanie dzienników zdarzeń do zewnętrznego serwera Syslog, • eksport informacji o przepływach sieciowych z wykorzystaniem protokołu sFlow, • synchronizację czasu z wykorzystaniem NTP lub SNTP, • pracę w trybie klienta DNS, • eksport, import i tworzenie kopii zapasowej konfiguracji, • aktualizację oprogramowania układowego, • możliwość pracy autonomicznej oraz zarządzania za pośrednictwem centralnego systemu zarządzania producenta.	
8	Architektura Dwa fizyczne urządzenie pełniące role zarządzanych urządzeń sieciowych, integrujących się i umożliwiających zarzadzanie bezpośrednio z dostarczanych urządzeń (NGFW NextGenFierwall), w ramach bieżącego postepowania.	
9	Gwarancja i wsparcie producenta Urządzenie musi zostać objęte aktywnym wsparciem producenta przez okres minimum 36 miesięcy od dnia odbioru, obejmującym co najmniej: • dostęp do aktualizacji oprogramowania układowego, • dostęp do portalu wsparcia producenta, • możliwość zgłaszania problemów bezpośrednio do pomocy technicznej producenta, • całodobowy dostęp do pomocy technicznej dla zgłoszeń krytycznych, • zaawansowaną wymianę uszkodzonego urządzenia w następnym dniu roboczym, zgodnie z warunkami świadczenia wsparcia producenta. • Wsparcie musi być zarejestrowane na Zamawiającego i możliwe do zweryfikowania w portalu producenta.	

16. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 1 szt

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Typ Obudowy: Punkt dostępowy przeznaczony do pracy wewnątrz pomieszczeń, wyposażony w anteny wewnętrzne. Obudowa w kolorze białym, przystosowana do montażu na ścianie lub suficie. Urządzenie musi zostać dostarczone z kompletem elementów niezbędnych do montażu.	
2	Porty: Urządzenie musi posiadać co najmniej: • 1 port 1/2,5 Gigabit Ethernet RJ45 z możliwością zasilania urządzenia przez PoE+, • 1 port konsolowy RJ45 umożliwiający lokalne zarządzanie i diagnostykę urządzenia.	
3	Obsługiwane pasma i parametry radiowe: Urządzenie musi posiadać minimum dwa niezależne moduły radiowe Wi-Fi oraz dodatkowy moduł komunikacji Bluetooth Low Energy. Urządzenie musi zapewniać: • pasmo 2,4 GHz: technologia 2×2 MIMO, szerokość kanału 20/40 MHz i maksymalna prędkość transmisji co najmniej 688 Mbps • pasmo 5 GHz: technologia 2×2 MIMO, szerokość kanału 20/40/80/160 MHz i maksymalna prędkość transmisji co najmniej 2,88 Gbps, • obsługę modulacji stosowanych w standardzie Wi-Fi 7, w tym 4096-QAM.	
4	Zasilanie: Zasilanie przez port Ethernet zgodnie ze standardem IEEE 802.3at PoE+. Maksymalny pobór mocy urządzenia nie może przekraczać 17 W. Jeżeli dostarczany przełącznik sieciowy nie zapewnia zasilania PoE+, Wykonawca musi dostarczyć dla każdego punktu dostępowego kompatybilny zasilacz lub injector PoE+ wraz z niezbędnym okablowaniem zasilającym.	
5	Funkcjonalności: Urządzenie musi zapewnić co najmniej: • obsługę standardów IEEE 802.11a/b/g/n/ac/ax/be, • obsługę zabezpieczeń WPA2-Personal, WPA2-Enterprise, WPA3-Personal oraz WPA3-Enterprise, • uwierzytelnianie użytkowników z wykorzystaniem standardu IEEE 802.1X i serwera RADIUS, • obsługę sieci VLAN zgodnie z IEEE 802.1Q oraz przypisywanie poszczególnych sieci SSID do sieci VLAN, • obsługę mechanizmów QoS/WMM oraz możliwość ograniczania przepustowości dla sieci bezprzewodowych lub podłączonych klientów, • izolację komunikacji pomiędzy klientami podłączonymi do tej samej sieci bezprzewodowej, • pracę sieci bezprzewodowej w trybie lokalnego mostu, tunelu oraz Mesh, • obsługę minimum 8 sieci SSID na każde radio obsługujące klientów,	

	• obsługę minimum 128 klientów bezprzewodowych na każde radio, • możliwość centralnego zarządzania za pomocą kontrolera sprzętowego, kontrolera wirtualnego lub systemu chmurowego producenta punktu dostępowego, • centralną konfigurację punktów dostępowych, sieci SSID, parametrów radiowych, zabezpieczeń oraz sieci VLAN, • monitorowanie stanu punktów dostępowych i podłączonych klientów, • aktualizację oprogramowania układowego za pośrednictwem centralnego systemu zarządzania. • Jeżeli centralne zarządzanie wymaga dodatkowej licencji lub subskrypcji, musi ona zostać dostarczona dla wszystkich oferowanych punktów dostępowych na okres minimum 36 miesięcy.	
6	Gwarancja i wsparcie producenta Urządzenie musi zostać objęte aktywnym wsparciem producenta przez okres minimum 36 miesięcy od dnia odbioru, obejmującym co najmniej: • dostęp do aktualizacji oprogramowania układowego, • dostęp do portalu wsparcia producenta, • możliwość zgłaszania problemów bezpośrednio do pomocy technicznej producenta, • całodobową pomoc techniczną dla zgłoszeń krytycznych, • zaawansowaną wymianę uszkodzonego urządzenia w następnym dniu roboczym, zgodnie z warunkami świadczenia wsparcia producenta. • Wsparcie musi być zarejestrowane na Zamawiającego i możliwe do zweryfikowania w portalu producenta.	

17. Oprogramowanie typu ITSM – 1 szt

Lp.	Parametry techniczne - wymagania minimalne	**Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)**
1	Dostawa i instalacja oprogramowania open-source klasy ITSM oraz oprogramowania do zarządzania aktualizacjami systemów w środowisku serwerowym Zamawiającego.	
2	Konfiguracja podstawowych parametrów systemowych rozwiązań, w tym adresacji IP, DNS oraz synchronizacji czasu NTP.	
3	Konfiguracja dostępu administracyjnego do konsoli zarządzającej systemu ITSM oraz systemu zarządzania aktualizacjami.	
4	Integracja systemu ITSM z usługą katalogową Microsoft Active Directory lub LDAP, jeżeli funkcjonalność ta jest dostępna w oferowanym rozwiązaniu.	
5	Konfiguracja ról, uprawnień oraz grup użytkowników administracyjnych i użytkowników końcowych w systemie ITSM.	

18. Oprogramowanie typu MDM – 1 szt

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Centralne zarządzanie smartfonami i tabletami z poziomu konsoli administracyjnej dostępnej przez przeglądarkę internetową.	
2	Instalacja serwera zarządzającego w infrastrukturze Zamawiającego, w modelu lokalnym.	
3	Licencja wieczysta, dla minimum 7 urządzeń. rozliczana na zarządzane urządzenie, obejmująca 12 miesięcy wsparcia technicznego producenta oraz dostępu do aktualizacji i poprawek. Wygaśnięcie wsparcia nie może powodować utraty prawa do użytkowania oprogramowania.	
4	Rejestracja i inwentaryzacja urządzeń, obejmująca informacje o modelu, systemie operacyjnym oraz zainstalowanych aplikacjach.	
5	Tworzenie grup urządzeń i zbiorcze przypisywanie im konfiguracji, aplikacji oraz polityk bezpieczeństwa.	
6	Wymuszanie polityk bezpieczeństwa, obejmujących wymagania dotyczące haseł, blokady ekranu oraz ograniczania funkcji urządzeń.	
7	Zdalne zarządzanie aplikacjami, obejmujące ich instalowanie, aktualizowanie i usuwanie.	
8	Centralna konfiguracja połączeń z sieciami bezprzewodowymi, połączeń VPN oraz dystrybucja certyfikatów.	
9	Możliwość zdalnego blokowania urządzeń oraz usuwania danych w przypadku ich utraty lub kradzieży.	
10	Generowanie raportów dotyczących zarządzanych urządzeń oraz rejestrowanie działań administratorów w dzienniku audytowym.	

19. Ochrona AntyDDos system typu DLP – 2 komplety

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	System musi być rozwiązaniem klasy DLP, przeznaczonym do ochrony przed nieuprawnionym wynoszeniem, kopiowaniem, przesyłaniem oraz udostępnianiem danych poza organizację.	
2	System musi być dostarczony w wersji instalowanej lokalnie w środowisku Zamawiającego, tj. w modelu on-premise.	
3	System musi posiadać centralną konsolę administracyjną dostępną z poziomu przeglądarki internetowej.	
4	System musi posiadać architekturę serwer–klient, w której centralny serwer zarządzający komunikuje się ze stacjami roboczymi za pośrednictwem zainstalowanych agentów.	
5	Serwer administracyjny systemu musi umożliwiać instalację na systemie Microsoft Windows Server 2019 lub nowszym.	
6	System musi wykorzystywać bazę danych Microsoft SQL Server lub Microsoft SQL Server Express do przechowywania konfiguracji, logów oraz zdarzeń.	
7	System musi umożliwiać ochronę co najmniej 7 stacji roboczych.	
8	Agent systemu DLP musi wspierać stacje robocze z systemami Microsoft Windows 10 oraz Microsoft Windows 11.	
9	System musi umożliwiać centralne zarządzanie agentami z poziomu konsoli administracyjnej, w tym podgląd statusu stacji roboczych oraz wersji zainstalowanego agenta.	
10	System musi umożliwiać integrację z usługą katalogową Microsoft Active Directory lub LDAP w celu synchronizacji użytkowników, grup oraz przypisywania polityk ochrony danych.	
11	System musi umożliwiać tworzenie polityk DLP dla użytkowników, grup użytkowników, stacji roboczych lub grup stacji roboczych.	
12	System musi umożliwiać pracę polityk DLP w trybach co najmniej: monitorowania/logowania, powiadamiania użytkownika oraz blokowania operacji.	
13	System musi umożliwiać kontrolę kopiowania plików na zewnętrzne nośniki danych, w tym pamięci USB oraz urządzenia pamięci masowej.	
14	System musi umożliwiać kontrolę przesyłania danych za pośrednictwem poczty elektronicznej, w tym kontrolę załączników oraz treści wiadomości.	
15	System musi umożliwiać kontrolę przesyłania plików przez przeglądarkę internetową, w tym przesyłania plików do poczty webowej, aplikacji webowych oraz serwisów internetowych.	
16	System musi umożliwiać kontrolę przesyłania danych do usług chmurowych, w tym co najmniej do usług typu OneDrive, SharePoint, Google Drive lub Dropbox.	
17	System musi umożliwiać kontrolę drukowania dokumentów oraz tworzenia wydruków do pliku.	
18	System musi umożliwiać kontrolę operacji kopiowania danych do schowka systemowego oraz wykonywania zrzutów ekranu dla danych objętych polityką ochrony.	
19	System musi umożliwiać kontrolę transferu plików w ramach połączeń zdalnych, w tym sesji RDP.	

20	System musi umożliwiać kontrolę przesyłania plików przez komunikatory internetowe lub aplikacje zaliczane do kategorii komunikacji.	
21	System musi umożliwiać klasyfikację danych w oparciu o typ pliku, lokalizację pliku, zawartość pliku, wzorce tekstowe oraz wyrażenia regularne.	
22	System musi umożliwiać wykrywanie danych wrażliwych, w tym numerów PESEL, numerów dokumentów, numerów rachunków bankowych IBAN, numerów kart płatniczych oraz innych ciągów znaków zdefiniowanych przez administratora.	
23	System musi posiadać mechanizm analizy zawartości plików w czasie wykonywania operacji objętych politykami DLP.	
24	System musi posiadać funkcjonalność OCR pozwalającą na analizę tekstu znajdującego się w obrazach, skanach lub dokumentach zawierających warstwę graficzną.	
25	Mechanizm OCR musi wspierać co najmniej polski zestaw znaków.	
26	System musi umożliwiać tworzenie własnych klasyfikacji danych oraz wykorzystanie ich w politykach ochrony danych.	
27	System musi umożliwiać prowadzenie audytu operacji na plikach, w tym informacji o użytkowniku, stacji roboczej, czasie zdarzenia, nazwie pliku, ścieżce źródłowej, miejscu docelowym oraz wykonanej akcji.	
28	System musi umożliwiać wykonanie kopii pliku powodującego naruszenie polityki DLP w celu późniejszej analizy incydentu.	
29	System musi umożliwiać generowanie alertów i powiadomień o naruszeniach polityk ochrony danych.	
30	System musi umożliwiać wysyłanie powiadomień e-mail do administratorów o wybranych zdarzeniach bezpieczeństwa lub incydentach DLP.	
31	System musi posiadać dashboardy lub widoki raportowe umożliwiające analizę incydentów, operacji na danych, aktywności użytkowników oraz wykorzystania kanałów transferu danych.	
32	System musi umożliwiać filtrowanie i analizę zdarzeń według co najmniej użytkownika, stacji roboczej, typu zdarzenia, kanału transferu danych, daty oraz poziomu istotności.	
33	System musi umożliwiać eksport danych raportowych lub zdarzeń do pliku w celu dalszej analizy lub archiwizacji.	
34	System musi umożliwiać konfigurację wyjątków od polityk DLP dla wskazanych użytkowników, grup, urządzeń, lokalizacji lub kanałów komunikacji.	
35	System musi umożliwiać definiowanie bezpiecznych oraz niezaufanych lokalizacji lub miejsc docelowych transferu danych.	
36	System musi umożliwiać zabezpieczenie konfiguracji przed nieuprawnioną zmianą poprzez role administracyjne oraz konta administracyjne.	
37	System musi umożliwiać rejestrowanie aktywności administratorów w konsoli zarządzającej.	
38	System musi umożliwiać aktualizację komponentów systemu oraz agentów zgodnie z mechanizmami udostępnianymi przez producenta oprogramowania.	
39	System musi posiadać dokumentację użytkową dostępną w języku polskim i angielskim.	
40	Wykonawca dostarczy licencję systemu DLP dla co najmniej 7 stacji roboczych wraz z prawem do aktualizacji, poprawek oraz wsparcia technicznego przez okres minimum 12 miesięcy.	

20. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT. – 1 komplet.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Usługa MDR (Managed Detection and Response) musi być świadczona jako rozszerzenie oferowanej w punkcie Oprogramowanie do ochrony przed ransomware ochrony antywirusowej oraz rozszerzenie oprogramowania EDR oferowanym w punkcie Oprogramowanie typu EDR (Endpoint Detection and Response) infrastruktury bezpieczeństwa Zamawiającego.	
2	Usługa musi zapewniać ciągłe monitorowanie środowiska Zamawiającego w trybie 24/7/365 oraz reagowanie na detekcje zgodnie z uprawnieniami uzgodnionymi wcześniej z Zamawiającym.	
3	Usługa musi być świadczona przez zespół bezpieczeństwa producenta systemu EDR, bez konieczności instalacji dodatkowego oprogramowania i reinstalacji agentów w środowisku Zamawiającego.	
4	Korzystanie z usługi nie może ograniczać administratorowi Zamawiającego dostępu do konsoli zarządzającej systemu EDR.	
5	Konsola służąca do komunikacji z analitykami i zarządzania środowiskiem musi posiadać interfejs w języku polskim.	
6	System musi na podstawie zebranych danych generować detekcje, stanowiące powiązane ze sobą podejrzane zdarzenia zarejestrowane przez agenta na stacjach roboczych i serwerach.	
7	W ramach usługi certyfikowani analitycy producenta muszą identyfikować potencjalne incydenty bezpieczeństwa poprzez walidację i badanie detekcji, w celu ustalenia czy incydent wymaga podjęcia dalszych działań naprawczych.	
8	Analitycy producenta muszą prowadzić ciągłą analizę oraz obsługę wygenerowanych detekcji, zapewniając ich kategoryzację i dokumentowanie co najmniej w zakresie oceny ryzyka, statusu badania zdarzeń oraz rejestrowania podejmowanych działań.	
9	Detekcje potwierdzone jako rzeczywiste zagrożenie muszą być eskalowane przez analityków producenta.	
10	Analitycy producenta muszą powiadomić osoby wyznaczone przez Zamawiającego do kontaktu niezwłocznie po wykryciu rzeczywistego incydentu.	
11	Po uzyskaniu upoważnienia Zamawiającego analitycy producenta muszą wykonywać działania: - ograniczające rozprzestrzenianie się zagrożenia, - zaradcze, - mające na celu przywrócenie normalnego działania środowiska.	
12	Zamawiający musi mieć możliwość określenia zakresu uprawnień analityków producenta do wykonywania działań reakcji w jego środowisku.	
13	Komunikacja z analitykami producenta w trakcie obsługi zdarzenia musi być dostępna co najmniej w sekcji komentarzy wykrytej detekcji w konsoli oraz telefonicznie.	
14	Po zneutralizowaniu zagrożenia analitycy producenta muszą przekazać Zamawiającemu rekomendacje dalszych działań, mających na celu zapobieżenie ponownemu wystąpieniu incydentu.	
15	Usługa musi umożliwiać dokupienie dodatkowych zasobów reagowania na	

	incydenty, objętych umową SLA, w przypadku wykrycia detekcji o podwyższonym poziomie zagrożenia dla środowiska Zamawiającego.	
16	Usługa musi obejmować co najmniej jedno urządzenie w okresie jej trwania i umożliwiać rozszerzenie zakresu o kolejne urządzenia w trakcie trwania umowy.	
17	Analitycy producenta nie mogą operować w krajach objętych sankcjami gospodarczymi, które uniemożliwiają realizację usług oraz będących krajami podwyższonego ryzyka związanego z nieuprawnionym pozyskiwaniem informacji.	
18	Wykonawca dostarczy usługę MDR dla co najmniej 7 urządzeń (stacji roboczych lub serwerów), na okres minimum 12 miesięcy.	
19	Usługi uruchomienia: - Aktywacja usługi MDR w konsoli zarządzającej dla urządzeń Zamawiającego. - Ustalenie i konfiguracja zakresu uprawnień analityków producenta do wykonywania działań reakcji. - Wskazanie i konfiguracja danych osób kontaktowych Zamawiającego na potrzeby powiadamiania o incydentach i eskalacji. - Weryfikacja poprawności przesyłania danych z agentów na wszystkich urządzeniach objętych usługą. - Instruktaż dla administratorów Zamawiającego w zakresie współpracy z analitykami producenta, obsługi komentarzy w detekcjach i procedury eskalacji.	

21. Oprogramowanie do zarządzania tożsamością i dostępem.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Oprogramowanie systemu operacyjnego Microsoft Windows Server 2025 Standard 16 Core - 1szt Licencja wieczysta umożliwiająca legalne użytkowanie oprogramowania systemu operacyjnego na oferowanym serwerze. Opis równoważności znajduje się pod tabelą. Zamawiający dopuszcza rozwiązanie OEM	

OPIS RÓWNOWAŻNOŚCI

1) Współpraca z procesorami o architekturze x86-64.
2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3) Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.
4) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2019.
5) Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
6) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
10) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
11) Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
12) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
13) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
14) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    – Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    – Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,

– Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.
– Zdalna dystrybucja oprogramowania na stacje robocze.
– Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
– PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - Dystrybucję certyfikatów poprzez http,
  - Konsolidację CA dla wielu lasów domeny,
  - Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.
– Szyfrowanie plików i folderów.
– Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
– Serwis udostępniania stron WWW.
– Wsparcie dla protokołu IP w wersji 6 (IPv6).
– Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
17) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
18) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
19) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania

22. Oprogramowanie typu MFA (dwu/wieloskładniwe uwierzytelnienie). – 6 szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Oprogramowanie lub sprzętowy klucz uwierzytelniający, zapewniający silne uwierzytelnianie dwuskładnikowe (2FA/MFA) oraz bezhasłowe logowanie. Interfejs: USB-C oraz obsługa NFC	
2	Protokoły uwierzytelniania: • FIDO2 / WebAuthn • FIDO U2F, • PIV (Smart Card), • OpenPGP, • OATH-TOTP/HOTP, • Challenge-Response, • Static Password.	
3	Kompatybilność: • Systemy operacyjne: Microsoft Windows, Apple macOS, Linux, ChromeOS, Android, iOS (przez USB-C). • Usługi: minimum Microsoft Entra ID,	
4	Odporność: spełniający standard IP68	
5	Certyfikaty: CE, RoHS, FCC, UKCA, FIDO Certified.	
6	Oferowany produkt musi być nowy, oryginalny, fabrycznie zapakowany, z pełną gwarancją producenta (minimum 12 miesięcy). Dostarczany z oryginalnym opakowaniem i instrukcją.	

23. Klucze sprzętowe U2F – 1 szt.

Lp.	Parametry techniczne - wymagania minimalne	**Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)**
1	Sprzętowy klucz uwierzytelniający, zapewniający silne uwierzytelnianie dwuskładnikowe (2FA/MFA) oraz bezhasłowe logowanie. Interfejs: USB-C oraz obsługa NFC	
2	Protokoły uwierzytelniania: • FIDO2 / WebAuthn • FIDO U2F, • PIV (Smart Card), • OpenPGP, • OATH-TOTP/HOTP, • Challenge-Response, • Static Password.	
3	Kompatybilność: • Systemy operacyjne: Microsoft Windows, Apple macOS, Linux, ChromeOS, Android, iOS (przez USB-C). • Usługi: minimum Microsoft Entra ID,	
4	Odporność: spełniający standard IP68	
5	Certyfikaty: CE, RoHS, FCC, UKCA, FIDO Certified.	
6	Oferowany produkt musi być nowy, oryginalny, fabrycznie zapakowany, z pełną gwarancją producenta (minimum 12 miesięcy). Dostarczany z oryginalnym opakowaniem i instrukcją.	

24. Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych) typ 1 - 2szt

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Zarządzalny sondy/przełącznik przemysłowy przeznaczony do komunikacji, segmentacji i monitorowania sieci OT. Urządzenie musi umożliwiać przekazywanie kopii wskazanego ruchu do sondy centralnego systemu IDS OT dostarczanego w ramach postępowania.	
2	Metalowa obudowa o stopniu ochrony minimum IP30, przystosowana do montażu na szynie DIN35. Dostawa musi obejmować również elementy umożliwiające zamontowanie urządzenia w szafie rack 19″, w tym odpowiedni adapter lub panel montażowy.	
3	Minimum 8 portów 10/100Base-T(X) RJ45, obsługujących autonegocjację prędkości, tryb Full/Half Duplex oraz automatyczne rozpoznawanie połączenia MDI/MDI-X.	
4	Tablica adresów MAC mieszcząca minimum 8000 wpisów, obsługa minimum 64 jednocześnie skonfigurowanych sieci VLAN oraz bufor pakietów o pojemności minimum 1 Mbit.	
5	Obsługa zasilania napięciem 24 V DC oraz możliwość podłączenia dwóch źródeł zasilania do redundantnych wejść urządzenia. Dla każdego przełącznika należy dostarczyć zasilacz 24 V DC przystosowany do zasilania z sieci 100–240 V AC, 50/60 Hz, wraz z wymaganym okablowaniem. Łącznie należy dostarczyć dwa zasilacze.	
6	Urządzenie musi obsługiwać co najmniej: VLAN zgodne z IEEE 802.1Q, VLAN przypisywane do portów, STP, RSTP, IGMP Snooping, LLDP oraz mechanizmy QoS umożliwiające priorytetyzację ruchu.	
7	Urządzenie musi obsługiwać Port Mirroring, umożliwiający kopiowanie ruchu z wybranych portów na port monitorujący podłączony do sondy IDS OT. Konfiguracja musi umożliwiać wskazanie monitorowanego kierunku ruchu. Dopuszcza się wykorzystanie jednego z wymaganych portów Ethernet jako portu monitorującego.	
8	Urządzenie musi umożliwiać udostępnianie informacji o swoim stanie i parametrach pracy z wykorzystaniem protokołów Modbus TCP oraz EtherNet/IP, na potrzeby zarządzania i monitorowania przełącznika.	
9	Urządzenie musi zapewniać zarządzanie przez interfejs WWW z wykorzystaniem HTTPS, dostęp administracyjny przez SSH oraz lokalny interfejs konsolowy. Dostawa musi obejmować kompatybilny przewód konsolowy. Wymagane są również funkcje zapisu i odtworzenia konfiguracji oraz aktualizacji oprogramowania układowego.	
10	Obsługa SNMPv1/v2c/v3, RMON, przekazywania dzienników zdarzeń do serwera Syslog oraz synchronizacji czasu przez NTP lub SNTP. Urządzenie musi umożliwiać sygnalizowanie wybranych zdarzeń za pomocą wiadomości e-mail lub wyjścia przekaźnikowego.	
11	Urządzenie musi zapewniać ochronę przed nadmiernym ruchem rozgłoszeniowym — Broadcast Storm Protection, blokowanie nieautoryzowanego dostępu do portów — Port Lock oraz ograniczanie dostępu administracyjnego do wskazanych adresów IP.	

12	Urządzenie musi być przystosowane do pracy w temperaturze obejmującej co najmniej zakres od −10°C do +60°C.	
13	Wykonawca musi zamontować i zasilić oba przełączniki, wykonać wymagane połączenia oraz skonfigurować adresację, VLAN, mechanizmy bezpieczeństwa i Port Mirroring. Musi zweryfikować poprawność przekazywania kopii ruchu do sond IDS oraz potwierdzić jej odbiór w dostarczanym systemie monitorowania OT.	
14	Dostawa musi obejmować dwa przełączniki, dwa zasilacze, komplet elementów montażowych, wymagane przewody oraz wszystkie licencje niezbędne do uruchomienia wskazanych funkcjonalności. Wymagane funkcje przełączników muszą być dostępne bez czasowego ograniczenia licencji.	
15	Przełączniki muszą zostać objęte gwarancją producenta przez minimum 36 miesięcy od odbioru końcowego. Dla zasilaczy należy zapewnić minimum 36 miesięcy gwarancji.	

25. Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych) typ 2 – 3szt

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Dedykowana sonda sprzętowa przeznaczona do pasywnego monitorowania komunikacji w sieciach automatyki przemysłowej OT/ICS/SCADA i przekazywania pozyskanych danych do centralnego systemu IDS, dostarczanego w ramach niniejszego zamówienia.	
2	Sonda musi być przystosowana do instalacji w szafach automatyki przemysłowej na szynie DIN35. Dostawa musi obejmować wszystkie elementy niezbędne do jej zamontowania.	
3	Sonda musi być przystosowana do zasilania napięciem 24 V DC. Dla każdej sondy należy dostarczyć dedykowany zasilacz umożliwiający podłączenie do instalacji Zamawiającego. Łączna dostawa musi obejmować trzy sondy i trzy zasilacze.	
4	Pozyskiwanie danych nie może powodować modyfikowania przesyłanych pakietów, generowania dodatkowego ruchu w monitorowanej sieci OT ani zakłócania komunikacji pomiędzy urządzeniami przemysłowymi.	
5	Sonda musi posiadać co najmniej jeden interfejs monitorujący RJ45 obsługujący Ethernet 10/100 Mbps, umożliwiający odbieranie kopii ruchu z portu SPAN/mirror przełącznika. Interfejs monitorujący musi być pozbawiony funkcji nadawania Tx i nie może identyfikować się w monitorowanej sieci poprzez adres MAC.	
6	Sonda musi posiadać pasywne interfejsy monitorujące RS232, RS422, RS485 oraz CAN, umożliwiające pozyskiwanie danych z sieci przemysłowych wykorzystujących te standardy komunikacji.	
7	Interfejsy monitorujące sieć OT oraz interfejs komunikacji z systemem centralnym muszą być odseparowane w sposób zapobiegający przenoszeniu nieautoryzowanego ruchu i zakłóceń pomiędzy monitorowaną siecią OT a siecią komunikacji z systemem IDS.	
8	Sonda musi umożliwiać szyfrowaną komunikację z centralnym systemem IDS. Interfejs komunikacyjny musi obsługiwać konfigurację statycznego adresu IP oraz pobieranie adresu z serwera DHCP.	
9	Sonda musi umożliwiać przekazywanie danych do centralnego systemu IDS w formacie IPFIX oraz ograniczanie przekazywanego ruchu co najmniej według wybranych urządzeń logicznych i protokołów.	
10	Sonda musi umożliwiać przechowywanie danych na karcie pamięci w postaci zaszyfrowanej z wykorzystaniem algorytmu co najmniej AES-128.	
11	Sonda musi wykrywać próbę otwarcia obudowy i przekazywać informację o takim zdarzeniu do centralnego systemu IDS w celu wygenerowania alarmu.	
12	Sonda musi umożliwiać zdalną zmianę konfiguracji oraz aktualizację oprogramowania układowego z wykorzystaniem centralnego systemu IDS.	
13	Wszystkie sondy wraz z dostarczonymi zasilaczami muszą zostać objęte gwarancją przez minimum 36 miesięcy od odbioru końcowego systemu. Sondy muszą posiadać wsparcie producenta obejmujące pomoc techniczną, dostęp do aktualizacji oprogramowania układowego oraz wymianę uszkodzonej sondy w przypadku awarii objętej gwarancją.	

26. Oprogramowanie/licencje IDS dedykowane sieciom OT — 1 szt.

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Oprogramowanie musi stanowić centralny system klasy IDS przeznaczony do monitorowania sieci automatyki przemysłowej OT/ICS/SCADA oraz wykrywania cyberzagrożeń, anomalii komunikacyjnych i nieprawidłowości operacyjnych. Rozwiązanie musi być niezależne od producentów monitorowanych urządzeń automatyki.	
2	Należy dostarczyć jedną licencję wieczystą typu site license, bez ograniczeń licencyjnych dotyczących liczby monitorowanych urządzeń i zasobów oraz liczby podłączonych sond w lokalizacji objętej licencją. Dostawa musi obejmować wszystkie licencje niezbędne do uruchomienia wymaganych funkcjonalności.	
3	Oprogramowanie musi umożliwiać jednoczesne zbieranie, korelowanie i analizowanie danych ze wszystkich trzech sond sprzętowych dostarczanych w pozycji „Sondy/sensory OT typ 2”. Musi umożliwiać późniejsze podłączanie kolejnych sond bez konieczności rozszerzania licencji oprogramowania centralnego.	
4	Oprogramowanie musi umożliwiać instalację w środowisku serwerowym Zamawiającego. Przetwarzanie analizowanego ruchu i przechowywanie danych systemu musi odbywać się w infrastrukturze Zamawiającego. Infrastrukturę serwerową, system operacyjny i środowisko wirtualizacyjne zapewnia Zamawiający.	
5	System musi posiadać interfejs graficzny dostępny przez przeglądarkę internetową, co najmniej w języku polskim i angielskim. Dostęp musi być zabezpieczony protokołem TLS, z możliwością importu własnego certyfikatu. System musi umożliwiać definiowanie poziomów uprawnień użytkowników.	
6	System musi analizować kopię ruchu pozyskiwaną przez sondy, bez generowania dodatkowego ruchu w monitorowanej sieci OT i bez modyfikowania komunikacji pomiędzy urządzeniami przemysłowymi. Musi obsługiwać dane przekazywane przez dostarczone sondy, w tym strumienie IPFIX.	
7	System musi automatycznie wykrywać urządzenia na podstawie obserwowanego ruchu, w tym sterowniki PLC, panele HMI, urządzenia RTU i IED oraz stacje operatorskie SCADA. Musi prezentować informacje o zasobach, identyfikować producenta co najmniej na podstawie adresu MAC oraz informować o pojawieniu się lub utracie urządzenia i zmianach komunikacji.	
8	System musi automatycznie tworzyć graficzną mapę urządzeń i połączeń komunikacyjnych. Mapa musi umożliwiać filtrowanie co najmniej według urządzeń, protokołów i portów oraz prezentować relacje pomiędzy urządzeniami. System musi uwzględniać informacje pozyskiwane z protokołów LLDP, CDP, CIP i SSDP.	
9	System musi realizować głęboką analizę pakietów DPI oraz interpretację komend i danych przesyłanych co najmniej w protokołach Modbus RTU i DNP3.	
10	System musi wspierać analizę z wykorzystaniem mechanizmów ML/AI co najmniej dla protokołów: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE.2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC 61850, SRTP i BACnet. Musi umożliwiać rozszerzenie obsługi o dodatkowe lub niestandardowe protokoły.	

11	System musi wykorzystywać uczenie maszynowe i mechanizmy analizy behawioralnej do modelowania charakterystyki monitorowanej sieci. Musi zapewniać ciągłe wykrywanie anomalii i alarmowanie w czasie rzeczywistym, również podczas budowania modelu sieci.	
12	System musi umożliwiać wykrywanie co najmniej: skanowania sieci i sterowników PLC, nietypowej częstotliwości komunikacji, niezgodności komend, nieautoryzowanych zmian komunikacji, połączeń z innymi sieciami oraz oznak ataków DoS/DDoS i Man-in-the-Middle.	
13	System musi identyfikować podatności wykrytych urządzeń i oprogramowania z wykorzystaniem informacji CVE pochodzących z baz MITRE lub NIST. Musi wspierać ocenę ryzyka, wskazywanie potencjalnych wektorów ataku oraz prezentowanie rekomendacji zwiększających bezpieczeństwo. Musi umożliwiać pasywne budowanie i utrzymywanie informacji o składnikach oprogramowania monitorowanej infrastruktury.	
14	System musi umożliwiać analizowanie plików PCAP, rejestrowanie monitorowanego ruchu oraz eksport wybranych pakietów do formatu PCAP. Musi umożliwiać konfigurację okresu przechowywania zdarzeń i archiwum ruchu. Pojemność przechowywanych danych nie może być ograniczana licencyjnie; może zależeć od dostępnych zasobów infrastruktury.	
15	System musi umożliwiać wykrywanie, rejestrowanie, analizowanie i klasyfikowanie incydentów oraz przypisywanie im priorytetów i statusów. Informacje o zdarzeniu muszą obejmować co najmniej opis techniczny, czas wystąpienia, uczestniczące urządzenia, poziom ważności i rekomendacje. Musi istnieć możliwość powiązania zdarzenia z zarejestrowanym ruchem oraz wysyłania powiadomień e-mail.	
16	System musi prezentować stan monitorowanej sieci, statystyki ruchu, zasoby, anomalie i incydenty w centralnych dashboardach. Musi umożliwiać generowanie raportów, zapamiętywanie widoków użytkownika oraz eksport zestawień urządzeń i wykrytych protokołów do CSV lub PDF, z informacją o podsieciach.	
17	System musi umożliwiać integrację z zewnętrznymi systemami SIEM co najmniej poprzez Syslog, synchronizację czasu przez NTP oraz aktualizację oprogramowania i baz podatności w trybie offline. Musi umożliwiać szyfrowaną komunikację z sondami, ich zdalną konfigurację i aktualizację oprogramowania układowego.	
18	Oprogramowanie musi zostać objęte wsparciem producenta przez minimum 36 miesięcy od odbioru końcowego systemu. Wsparcie musi obejmować przyjmowanie zgłoszeń, pomoc techniczną, dostęp do dokumentacji oraz nowych wersji, aktualizacji i poprawek oprogramowania.	
19	Wykonawca musi zainstalować, zalicencjonować i skonfigurować oprogramowanie centralne, zintegrować je z trzema dostarczonymi sondami oraz skonfigurować monitorowane sieci, protokoły, mechanizmy detekcji, alarmowanie, dashboardy i raporty. Prace muszą zostać uzgodnione z Zamawiającym i nie mogą zakłócać działania monitorowanej infrastruktury OT.	
20	Wykonawca musi zweryfikować poprawność zbierania i analizowania danych ze wszystkich trzech sond oraz przeprowadzić testy funkcjonalne systemu. Przed odbiorem końcowym musi przekazać dokumentację powykonawczą, opis konfiguracji oraz dane dostępowe i administracyjne.	

27. UTM (Unified Threat Management) – 1szt.

Lp.	Parametry techniczne - wymagania minimalne	**Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)**
1	Wymagania ogólne System bezpieczeństwa musi być dostarczony w postaci dedykowanego urządzenia sprzętowego. System musi realizować funkcje sieciowe i bezpieczeństwa niezależnie od operatora i rodzaju wykorzystywanego łącza. System musi umożliwiać pracę co najmniej w trybach: • routera z funkcją NAT, • transparentnym, • monitorowania ruchu przekazywanego z portu SPAN lub TAP. System musi obsługiwać protokoły IPv4 oraz IPv6 w zakresie zapory sieciowej, routingu, połączeń VPN i mechanizmów ochronnych. System musi umożliwiać definiowanie kont administracyjnych i przydzielanie im uprawnień do poszczególnych instancji lub części konfiguracji.	
2	Redundancja i monitorowanie System musi umożliwiać łączenie dwóch urządzeń w klaster wysokiej dostępności pracujący w trybie Active-Passive lub Active-Active. Klaster musi umożliwiać synchronizację konfiguracji i aktywnych sesji firewall. System musi monitorować stan urządzenia, interfejsów, połączeń sieciowych oraz tuneli VPN. System musi umożliwiać agregację interfejsów statycznie oraz z wykorzystaniem protokołu LACP. System musi umożliwiać tworzenie interfejsów redundantnych. W przypadku dostarczenia klastra wszystkie urządzenia muszą być objęte jednakowym zakresem licencji i wsparcia producenta.	
3	Interfejsy i zasilanie Urządzenie musi posiadać co najmniej: • 4 portów 10/100/1000Base-T RJ45, • port konsolowy umożliwiający lokalne zarządzanie, Wszystkie wymagane porty sieciowe muszą umożliwiać równoczesną pracę. System musi pozwalać na skonfigurowanie interfejsów wirtualnych VLAN zgodnych z IEEE 802.1Q. Urządzenie musi być wyposażone w zasilanie AC wraz z zasilaczem i przewodem umożliwiającym podłączenie do instalacji Zamawiającego.	
4	Parametry wydajnościowe System musi zapewniać co najmniej: • obsługę 600 000 jednoczesnych sesji firewall, • obsługę 30 000 nowych sesji na sekundę, • przepustowość Stateful Firewall dla pakietów 512 B - 4 Gbps, • przepustowość kontroli aplikacji – 830 Mbps, • przepustowość IPsec VPN dla pakietów 512 B - 3,5 Gbps, • przepustowość IPS – 800Mbps, • przepustowość NGFW - 570 Mbps, • przepustowość ochrony przed zagrożeniami dla ruchu Enterprise Traffic	

	Mix, z włączonymi funkcjami Firewall, IPS, kontroli aplikacji i ochrony przed malware – 500 Mbps, • przepustowość inspekcji komunikacji SSL/TLS - 400 Mbps. Wartości muszą być potwierdzone w publicznie dostępnej dokumentacji producenta.	
5	Podstawowe funkcje bezpieczeństwa System musi realizować co najmniej: • zaporę sieciową klasy Stateful Inspection, • kontrolę aplikacji, • szyfrowane połączenia IPsec VPN, • ochronę antywirusową i przed malware, • ochronę IPS, • zarządzanie pasmem, QoS i Traffic Shaping, • inspekcję ruchu szyfrowanego SSL/TLS, • uwierzytelnianie wieloskładnikowe z wykorzystaniem tokenów sprzętowych lub programowych, • automatyczne wykonywanie zdefiniowanych akcji po wystąpieniu określonego zdarzenia bezpieczeństwa.	
6	Polityki firewall i NAT Polityki firewall muszą umożliwiać uwzględnienie co najmniej: • źródłowych i docelowych adresów IP, • użytkowników i grup użytkowników, • interfejsów oraz stref bezpieczeństwa, • protokołów i usług, • aplikacji lub kategorii aplikacji, • harmonogramów, • profili bezpieczeństwa, • rejestrowania zdarzeń. System musi obsługiwać: • źródłową i docelową translację adresów, • PAT, • translację jeden do jednego oraz jeden do wielu, • dedykowany ALG dla protokołu SIP. System musi umożliwiać tworzenie stref bezpieczeństwa, np. LAN, WAN i DMZ. System musi umożliwiać filtrowanie ruchu na podstawie kraju przypisanego do źródłowego lub docelowego adresu IP. System musi umożliwiać korzystanie z zewnętrznych źródeł zawierających adresy IP, domeny lub adresy URL. System musi pozwalać na określenie czasu aktywności poszczególnych reguł firewall.	
7	System musi obsługiwać co najmniej: • IKEv1 oraz IKEv2, • szyfrowanie AES-128 i AES-256, w tym tryb GCM, • grupy Diffie-Hellman co najmniej 19 i 20, • tunele Site-to-Site oraz Client-to-Site, • topologie Hub-and-Spoke oraz Mesh, • uwierzytelnianie kluczem współdzielonym i certyfikatem, • routing statyczny i dynamiczny przez tunele VPN, • IPsec NAT Traversal, DPD i XAuth, • mechanizm Split Tunneling,	

	• monitorowanie dostępności tuneli i automatyczne uruchamianie tunelu zapasowego, • ograniczanie liczby jednocześnie negocjowanych tuneli w celu ochrony zasobów systemu. • Producent musi posiadać w ofercie oprogramowanie klienckie umożliwiające zestawianie połączeń VPN.	
8	Routing, SD-WAN i zarządzanie pasmem System musi obsługiwać: • routing statyczny, • Policy Based Routing, • RIPv2 i RIPng, • OSPF i OSPFv3, • BGP, • PIM, • filtrowanie tras, • ECMP, • BFD. System musi monitorować dostępność wskazanego adresu IP i automatycznie modyfikować tablicę routingu po wykryciu awarii. Mechanizm SD-WAN musi obsługiwać interfejsy fizyczne i wirtualne, w tym VLAN oraz IPsec. System musi umożliwiać wybór łącza na podstawie parametrów jakościowych, dostępności oraz zdefiniowanych reguł. Zarządzanie pasmem musi umożliwiać: • określenie pasma maksymalnego i gwarantowanego, • określenie priorytetu ruchu, • oznaczanie DSCP.	
9	Ochrona przed malware • System musi skanować ruch w obu kierunkach, również dla aplikacji pracujących na niestandardowych portach. • Skanowanie musi obejmować co najmniej HTTP, HTTPS, FTP, POP3, IMAP, SMTP i CIFS. • System musi posiadać sygnatury malware dla urządzeń mobilnych, co najmniej dla systemu Android. • Bazy sygnatur muszą być aktualizowane automatycznie. • System musi wykorzystywać mechanizmy heurystyczne i uczenie maszynowe do wykrywania zagrożeń. • Administrator musi mieć możliwość zastosowania ochrony antywirusowej wyłącznie dla wybranych polityk i zakresów ruchu.	
10	Ochrona IPS i kontrola aplikacji • Ochrona IPS musi wykorzystywać analizę sygnaturową oraz analizę anomalii protokołów. • System musi chronić aplikacje działające na standardowych i niestandardowych portach. • Baza IPS musi zawierać minimum 5000 sygnatur i być aktualizowana automatycznie. • Administrator musi mieć możliwość definiowania własnych sygnatur i wyjątków. • System musi wykrywać anomalie ruchu oraz zapewniać ochronę przed atakami DoS i DDoS.	

	• System musi wykrywać i blokować komunikację z sieciami botnet i serwerami C&C. • Funkcje IPS muszą być przypisywane do wybranych polityk firewall. • Kontrola aplikacji musi wykorzystywać głęboką analizę pakietów i nie może bazować wyłącznie na numerach portów TCP/UDP. • Baza kontroli aplikacji musi zawierać minimum 2000 sygnatur. • System musi umożliwiać blokowanie aplikacji typu proxy i P2P oraz aplikacji wykorzystujących niestandardowe porty.	
11	Uwierzytelnianie użytkowników System musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: • lokalnej bazy użytkowników, • LDAP i Microsoft Active Directory, • RADIUS, • zewnętrznych systemów uwierzytelniania, • protokołu SAML. System musi umożliwiać integrację z Active Directory w celu realizacji Single Sign-On. Tożsamość użytkownika lub grupy musi być możliwa do wykorzystania bezpośrednio w politykach firewall. System musi umożliwiać stosowanie uwierzytelniania dwuskładnikowego dla administratorów oraz użytkowników połączeń VPN.	
12	Zarządzanie i diagnostyka System musi umożliwiać lokalne zarządzanie poprzez HTTPS i SSH. System musi umożliwiać współpracę z centralnymi platformami zarządzania i monitorowania producenta. System musi obsługiwać: • SNMPv2c i SNMPv3, • NetFlow lub sFlow, • API z publicznie dostępną dokumentacją. System musi posiadać narzędzia diagnostyczne obejmujące co najmniej ping, traceroute, przechwytywanie pakietów oraz diagnostykę sesji firewall. System musi umożliwiać: • uwierzytelnianie dwuskładnikowe administratorów, • tworzenie profili administracyjnych o różnych uprawnieniach, • ograniczenie dostępu administracyjnego do wskazanych adresów źródłowych, System musi umożliwiać współpracę z centralną platformą zarządzania producenta, pozwalającą na realizację zmian konfiguracyjnych w trybie workflow, z ich zatwierdzaniem przed zastosowaniem.	
13	Logowanie System musi rejestrować co najmniej: • ruch zaakceptowany i zablokowany, • aktywność administratorów, • zdarzenia modułów bezpieczeństwa, • wykorzystanie zasobów, • stan pracy urządzenia. System musi umożliwiać włączenie lub wyłączenie logowania dla każdej reguły firewall. System musi umożliwiać jednoczesne przekazywanie logów do wielu zewnętrznych systemów.	

	System musi obsługiwać protokół SYSLOG, w tym transmisję przez TCP oraz komunikację szyfrowaną SSL/TLS.	
14	Licencje Dla urządzenia należy dostarczyć aktywne licencje bezpieczeństwa na okres minimum 12 miesięcy, obejmujące co najmniej: • aktualizacje kontroli aplikacji, • aktualizacje IPS, • ochronę antywirusową i Advanced Malware Protection,	
15	Gwarancja i wsparcie producenta Urządzenie musi zostać objęte aktywnym wsparciem producenta przez okres minimum 12 miesięcy od dnia odbioru. Wsparcie musi obejmować co najmniej: • pomoc techniczną producenta w trybie 24×7×365, • czas reakcji dla zgłoszeń krytycznych nie dłuższy niż 1 godzina, • dostęp do aktualizacji oprogramowania systemowego, • dostęp do portalu wsparcia i narzędzi producenta, • możliwość zgłaszania problemów przez portal internetowy i telefonicznie, • zaawansowaną wymianę uszkodzonego urządzenia w trybie AHR, zgodnie z warunkami producenta. • Licencje i wsparcie muszą być widoczne na koncie Zamawiającego.	

28. Usługa Private APN – 5 szt

Lp.	Parametry techniczne - wymagania minimalne	Producent: …… Model: …… Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Usługa lub modem sprzętowy umożliwiający komunikacje LTE lub 5G	
2	Obsługa kart SIM lub nanoSIM	
3	Interfejs: USB 2.0 lub nowszy,	
4	Gwarancja: 24 miesiące	

29. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 1szt.

Lp.	Parametry techniczne - wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Typ obudowy: Obudowa do montażu w szafie RACK 19” – 2U wraz z zestawem montażowym.	
2	Typ urządzenia: 1-fazowy	
3	Moc urządzenia: Minimum 2000W (2000 VA)	
4	Gniazdo zasilania (wejścia): IEC320-C20 – 16A	
5	Gniazda wyjściowe: - min. 4x IEC320-C13 - min. 4x IEC320-C13 (programowalne)	
6	Minimalny czas podtrzymania bateryjnego dla 70% mocy nominalnej: 10 minut. Zamawiający dopuszcza użycie dodatkowej baterii w obudowie do montażu w szafie RACK 19” o wysokości 2U.	
7	Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o: • Stan UPS, • Wejście bypassu, • Stan baterii, • Wejście sieci podstawowej, • Przycisk ESC, • Przycisk nawigacyjny • Przycisk WŁ./WYŁ. • Wyjście • Poziom obciążenia, Pasek wskaźników diodowych LED	
8	Zasilacz UPS musi być wyposażony w port RS232 (do obsługi protokołu MODBUS), Zasilacz musi być wyposażony w kartę komunikacyjną posiadającą poniższe funkcje oraz parametry: • połączenie z siecią Ethernet 10/100 Mb/s oraz 1Gb/s (złącze RJ 45), • monitorowanie zasilacza UPS za pomocą przeglądarki internetowej, • zdalne wyłączanie serwerów autonomicznych lub działających środowisku wirtualnym • informacja o awariach wysyłana e-mailem • zarządzanie zasilaczem UPS za pomocą protokołu SNMP, • Modbus TCP • Protokół HTTPS	
9.	Gwarancja: minimum 24 miesiące	

30. Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT zamawiającego, zakres zostanie ustalony po przygotowaniu projektu wdrożenia.	

31. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IoT

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Przygotowanie projektu wdrożenia rozwiązania z zakresu bezpieczeństwa biorąc pod uwagę dostarczone urządzania, oprogramowanie oraz usługi w zakresie obszaru OT	

32. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu OpenSource IT/OT/ICS/IIoT

A. Usługi w zakresie dostawy urządzenia Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA oraz Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA

- Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
- Okablowanie sieciowe urządzeń (sieć LAN oraz SAN)
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
- Uruchomienie i weryfikacja poprawności działania urządzeń
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
- Konfiguracja adresacji IP interfejsów zarządzania
- Konfiguracja protokołu synchronizacji czasu NTP
- Konfiguracja protokołu rozwiązywania nazw DNS
- Weryfikacja poprawności działania połączeń LAN
- Weryfikacja poprawności działania połączeń SAN
- Wykonanie testów działania nadmiarowości zasilania i odporności na zanik napięcia w jednym źródle zasilania
- Konfiguracja wirtualnych sieci VLAN,
- Konfiguracja drzewa rozpinającego na podłączanych do serwera portach,
- Konfiguracja mechanizmów bezpieczeństwa na przełącznikach sieciowych,
- Weryfikacja poprawności dziania komunikacji z serwerem w przypadku pojedynczego awarii połączenia,
- Instalacja oprogramowania wirtualizacyjnego – Hyper-V
- Konfiguracja sieci zarządzania IP,
- Konfiguracja wirtualnej sieci VLAN,
- Konfiguracja protokołu synchronizacji czasu NTP dla oprogramowania wirtualizacyjnego
- Konfiguracja protokołu rozwiązywania nazw DNS dla oprogramowania wirtualizacyjnego
- Konfiguracja wirtualnych przełączników,
- Konfiguracja dedykowanej wirtualnej sieci dla migracji wirtualnych maszyn,
- Instalacja wirtualnej maszyny z oprogramowaniem Windows Server 2025,
- Konfiguracja i podłączenie wdrożonych wirtualnych maszyn do skonfigurowanych wirtualnych przełączników,
- Zastosowanie najlepszych praktyk w celu zabezpieczenia wirtualnych maszyn na poziomie wirtualizatora,

B. Usługi w zakresie wdrożenia Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X(Switch) – 1 komplet

- Zaprojektowanie segmentacji sieci LAN,
- Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
- Okablowanie sieciowe urządzeń sieć LAN
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
- Uruchomienie i weryfikacja poprawności działania urządzeń
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
- Konfiguracja adresacji IP interfejsów zarządzania
- Konfiguracja protokołu synchronizacji czasu NTP
- Konfiguracja protokołu rozwiązywania nazw DNS
- Weryfikacja poprawności działania połączeń LAN

- Wykonanie testów działania nadmiarowości zasilania i odporności na zanik napięcia w jednym źródle zasilania
- Wdrożenie sieci wirtualnych – segmentacja,
- Konfiguracja połączeń agregowanych,
- Konfiguracja protokołów drzewa rozpinającego,

C. Wdrożenie w zakresie Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 1szt.

- Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
- Okablowanie sieciowe urządzeń sieć LAN
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
- Uruchomienie i weryfikacja poprawności działania urządzeń
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
- Konfiguracja adresacji IP interfejsów zarządzania
- Konfiguracja protokołu synchronizacji czasu NTP
- Konfiguracja protokołu rozwiązywania nazw DNS
- Weryfikacja poprawności działania połączeń LAN
- Weryfikacja poprawności działania przełączania bateryjnego w przypadku awarii prądu.

D. Wdrożenie dostarczanego NGFW (Next Gen FireWall), oraz UTM (Unified Threat Management) – 1szt

- Instalacja dostarczonego klastra UTM w miejscu wyznaczonym przez Zamawiającego,
- Podłączenie urządzeń do sieci zasilania,
- Aktualizacja oprogramowania systemowego urządzeń do najwyższej rekomendowanej przez producenta wersji,
- Konfiguracja konstrukcji klastra wysokiej dostępności pracującego w trybie Active/Passive
- Konfiguracja adresacji sieciowej IPv4,
- Konfiguracja protokołu rozpoznawania nazw DNS,
- Konfiguracja protokołu synchronizacji czasu NTP,
- Konfiguracja protokołu logowania zdarzeń syslog,
- Konfiguracja i przygotowanie banneru logowania, zgodnie z wymaganiami Zamawiającego,
- Wdrożenie skonfigurowanego klastra UTM w sieci Zamawiającego,
- Zaprojektowanie polityk bezpieczeństwa zgodnych z wymaganiami Zamawiającego,
- Implementacja polityk bezpieczeństwa wraz z wymaganymi modułami skanującymi,
- Implementacja dodatkowych rekomendowanych polityk bezpieczeństwa zgodnymi z najlepszymi praktykami dotyczącymi zabezpieczenia infrastruktury.
- Wdrożenie polityk typu port-forwarding w celu udostępnienia zasobów lokalnych/usług na zewnątrz.
- Konfiguracja sieci VPN pomiędzy lokalizacjami, zgodnie z wymaganiami Zamawiającego,
- Konfiguracja grup użytkowników w domenie MS Active Directory, na potrzeby klienckiej sieci VPN,
- Konfiguracja sieci VPN dla użytkowników końcowych typu VPN (Client-To-Site)
- Konfiguracja połączeń WAN(Dostęp do Internetu) jako Multi-WAN – możliwość korzystania z kilku operatorów sieci jednocześnie.
- Konfiguracja połączeń agregowanych z wykorzystaniem protokołu LACP,
- Wdrożenie wymaganych polityk bezpieczeństwa pomiędzy sieciami lokalnymi (VLAN)
- Integracja z domeną MS Active Directory,
- Wdrożenie narzędzia Single Sign On(SSO) wraz z przygotowaniem polityki GPO w domenie MS Active Directory oraz implementacja na stacjach roboczych,
- Wdrożenie mechanizmu deszyfracji połączeń zaszyfrowanych, wraz z implementacja modułów skanujących i chroniących przed atakami typu Zero-Day,

- Konfiguracja logowania zdarzeń dla polityk bezpieczeństwa,
- Integracja z serwerem poczty,
- Konfiguracja powiadomień oraz alarmów,

E. Usługi w zakresie dostawy i wdrożenia Network Attached Storage (NAS)

- Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
- Okablowanie sieciowe urządzeń (sieć LAN oraz SAN)
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
- Uruchomienie i weryfikacja poprawności działania urządzeń
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
- Konfiguracja adresacji IP interfejsów zarządzania
- Konfiguracja protokołu synchronizacji czasu NTP
- Konfiguracja protokołu rozwiązywania nazw DNS
- Weryfikacja poprawności działania połączeń LAN
- Weryfikacja poprawności działania połączeń SAN
- Konfiguracja wirtualnych sieci VLAN,
- Konfiguracja drzewa rozpinającego na podłączanych do serwera portach,
- Konfiguracja mechanizmów bezpieczeństwa na przełącznikach sieciowych,
- Konfiguracja przestrzeni dyskowej,
- Konfiguracja mechanizmów systemu kopii zapasowej,
- Wykonanie kopii zapasowej.

F. Usługi w zakresie sieci bezprzewodowej Wi-Fi

- Podłączenie urządzenia do sieci zasilania zgodnie z wytycznymi Zamawiającego,
- Inicjalizacja punktów dostępowych,
- Okablowanie sieciowe urządzenia,
- Uruchomienie i weryfikacja poprawności działania urządzeń,
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
- Konfiguracja adresacji IP interfejsów zarządzania,
- Konfiguracja protokołu synchronizacji czasu NTP,
- Konfiguracja protokołu rozwiązywania nazw DNS,
- Konfiguracja wirtualnych sieci VLAN,
- Konfiguracja sieci bezprzewodowych,

G. Wdrożenie domeny Microsoft Active Directory

- Przygotowanie architektury usługi katalogowej Active Directory w oparciu o dwie wirtualne maszyny uruchomione na dostarczanych serwerach.
- Instalacja systemu Microsoft Windows Server 2025 Datacenter na dwóch wirtualnych maszynach przeznaczonych do pełnienia roli kontrolerów domeny.
- Instalacja i konfiguracja ról Active Directory Domain Services, DNS oraz DHCP na wirtualnych maszynach pełniących funkcję kontrolerów domeny.
- Utworzenie nowej domeny Active Directory zgodnie z nazwą i strukturą uzgodnioną z Zamawiającym.
- Konfiguracja dwóch kontrolerów domeny Active Directory pracujących redundantnie w ramach jednej domeny.
- Konfiguracja adresacji IP interfejsów sieciowych kontrolerów domeny.
- Konfiguracja protokołu synchronizacji czasu NTP dla kontrolerów domeny.
- Konfiguracja usługi DNS na potrzeby prawidłowego działania domeny Active Directory.
- Konfiguracja usługi DHCP dla wskazanych przez Zamawiającego podsieci IP.
- Konfiguracja podstawowej struktury jednostek organizacyjnych OU dla użytkowników, komputerów, serwerów oraz grup zabezpieczeń.
- Utworzenie kont użytkowników domenowych wskazanych przez Zamawiającego.

- Utworzenie podstawowych grup zabezpieczeń oraz przypisanie użytkowników do odpowiednich grup zgodnie z wytycznymi Zamawiającego.
- Dołączenie wskazanych stacji roboczych i/lub serwerów do domeny Active Directory.
- Przygotowanie i wdrożenie podstawowych zasad Group Policy Object, w tym zasad haseł, blokady kont oraz podstawowych ustawień bezpieczeństwa.
- Weryfikacja poprawności działania logowania użytkowników do domeny oraz dostępu do zasobów zgodnie z przypisanymi uprawnieniami.
- Przeprowadzenie testów funkcjonalnych wdrożonego rozwiązania, obejmujących logowanie użytkownika domenowego, działanie replikacji Active Directory, działanie DNS, działanie DHCP, działanie zasad GPO oraz poprawność członkostwa komputerów w domenie.

H. Przygotowanie dokumentacji powykonawczej, która zawierać będzie co najmniej:

- Topologia fizyczna,
- Topologia logiczna,
- Adresacja IP,
- Konfiguracja komponentów, systemów i urządzeń,
- Poświadczenia dostępowe,
- Procedury wykonywania oraz odzyskiwania kopii zapasowych.

33. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Wykonanie testów bezpieczeństwa dostępu do sieci IT/OT/ICSC/IIoT – scenariusz testów zostanie uwzględniony w projekcie wdrożenia.	

34. Szkolenie z zakresu Cyberbezpieczeństwo – szkolenie specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowana) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Zamawiający wymaga przeprowadzenia szkolenia z zakresu Cyberbezpieczeństwo oraz dostarczonego i wdrożonego rozwiązania. Czas trwania 3 dni Ilość osób: 2	

35. Szkolenia z zakresu cyberbezpieczeństwa kadry, istotnych z punktu widzenia wdrażanej Polityki Bezpieczeństwa Informacji i Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Czas trwania: 6 godzin lekcyjnych (6 × 45 minut), bez uwzględnienia przerw.	
2	Forma szkolenia: stacjonarna lub zdalna (online), uzgodniona z Zamawiającym.	
3	Zakres tematyczny szkolenia a) Podstawy cyberbezpieczeństwa i SZBI (1 godz.) – zasady bezpieczeństwa informacji, wymagania ISO/IEC 27001, odpowiedzialność kadry kierowniczej i pracowników. b) Polityka Bezpieczeństwa Informacji (1 godz.) – ochrona informacji i danych osobowych, zarządzanie dostępem, obowiązki pracowników i stosowanie procedur SZBI. c) Cyberzagrożenia w środowiskach IT i OT (1 godz.) – najczęstsze ataki, phishing, ransomware, złośliwe oprogramowanie, kradzież danych, ataki na systemy SCADA/ICS i infrastrukturę przemysłową. d) Identyfikacja zagrożeń i działania zapobiegawcze (1 godz.) – rozpoznawanie prób cyberataków, podejrzanych wiadomości, nieuprawnionego dostępu i nieprawidłowego działania systemów, zasady bezpiecznego korzystania z zasobów IT i OT. e) Incydenty bezpieczeństwa i ciągłość działania (1 godz.) – rozpoznawanie i zgłaszanie incydentów, zasady reagowania, ograniczanie skutków cyberataków oraz podstawy zachowania ciągłości działania. f) Praktyczne przykłady zagrożeń i podsumowanie (1 godz.) – przykłady cyberataków na środowiska IT i OT, sposoby postępowania, dobre praktyki oraz test wiedzy.	
4	Wymagania dotyczące realizacji szkolenia a) Szkolenie należy przeprowadzić w formie wykładu z wykorzystaniem praktycznych przykładów cyberzagrożeń. b) Program szkolenia należy dostosować do specyfiki działalności Zamawiającego oraz wdrażanej Polityki Bezpieczeństwa Informacji i SZBI. c) Wykonawca zapewni materiały szkoleniowe w formie elektronicznej. d) Szkolenie stacjonarne lub online musi umożliwiać uczestnikom zadawanie pytań prowadzącemu. e) Po zakończeniu szkolenia należy przeprowadzić test sprawdzający wiedzę uczestników.	
5	Dokumentacja i odbiór szkolenia Wykonawca przekaże Zamawiającemu: a) Program i materiały szkoleniowe. b) Listę obecności lub potwierdzenie uczestnictwa. c) Wyniki testu wiedzy. d) Zaświadczenia lub certyfikaty uczestnictwa. Warunkiem odbioru zamówienia jest przeprowadzenie szkolenia w wymiarze 6 godzin lekcyjnych, zgodnie z określonym zakresem oraz przekazanie wymaganej dokumentacji.	

36. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, weryfikującymi świadomość zagrożeń i reakcje personelu, w szczególności osób realizujących obowiązki w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z przyjętymi procedurami

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Czas trwania szkolenia: 6 godzin lekcyjnych (6 × 45 minut), bez uwzględnienia przerw.	
2	Forma szkolenia: stacjonarna lub zdalna (online), uzgodniona z Zamawiającym.	
3	Zakres tematyczny szkolenia a) Podstawy zagrożeń socjotechnicznych (1 godz.) – rodzaje ataków, phishing, spear phishing, smishing, vishing, podszywanie się pod pracowników i przełożonych oraz metody manipulacji. b) Identyfikacja zagrożeń socjotechnicznych (1 godz.) – rozpoznawanie podejrzanych wiadomości, odnośników, załączników, prób wyłudzenia informacji i danych uwierzytelniających. c) Zagrożenia socjotechniczne w środowiskach IT i OT (1 godz.) – ataki ukierunkowane na pracowników, administratorów i personel techniczny, zagrożenia związane z dostępem do systemów i infrastruktury organizacji. d) Zasady reagowania na zagrożenia (1 godz.) – zgłaszanie podejrzanych zdarzeń, postępowanie w przypadku próby oszustwa, ochrona informacji oraz działania zgodne z procedurami SZBI. e) Reagowanie na incydenty w ramach SZBI (1 godz.) – obowiązki osób odpowiedzialnych za bezpieczeństwo informacji, przyjmowanie i kwalifikowanie zgłoszeń, eskalacja, dokumentowanie zdarzeń oraz podejmowanie działań zgodnie z przyjętymi procedurami. f) Analiza testów socjotechnicznych i podsumowanie (1 godz.) – omówienie scenariuszy zagrożeń, analiza zachowań pracowników, najczęstsze błędy, prawidłowe reakcje i działania zapobiegawcze.	
4	Zakres testów socjotechnicznych a) Przygotowanie i przeprowadzenie symulowanych ataków socjotechnicznych, w szczególności kampanii phishingowych. b) Przeprowadzenie testów przed szkoleniem oraz po jego zakończeniu w celu porównania poziomu świadomości zagrożeń. c) Weryfikacja umiejętności rozpoznawania zagrożeń oraz prawidłowości reakcji pracowników. d) Sprawdzenie sposobu zgłaszania i obsługi symulowanych incydentów przez osoby realizujące obowiązki w ramach SZBI, zgodnie z obowiązującymi procedurami. e) cena prawidłowości eskalacji, dokumentowania zgłoszeń i podejmowania działań przez wyznaczony personel. f) Opracowanie raportu z wyników testów, zidentyfikowanych słabości i zaleceń dotyczących poprawy świadomości oraz skuteczności reagowania.	
5	Wymagania dotyczące realizacji szkolenia i testów a) Program szkolenia i scenariusze testów należy dostosować do specyfiki działalności Zamawiającego oraz obowiązujących procedur SZBI. b) Zakres i zasady przeprowadzania testów muszą zostać uzgodnione z	

	Zamawiającym. c) Testy nie mogą powodować zakłóceń działania systemów IT i OT ani wymagać pozyskiwania rzeczywistych haseł użytkowników. d) Wykonawca zapewni materiały szkoleniowe w formie elektronicznej. e) Szkolenie musi umożliwiać uczestnikom zadawanie pytań prowadzącemu. f) Wykonawca przedstawi wyniki testów i rekomendacje dotyczące działań doskonalących.	
6	Dokumentacja i odbiór zamówienia Wykonawca przekaże Zamawiającemu: a) Program i materiały szkoleniowe. b) Listę obecności lub potwierdzenie uczestnictwa. c) Opis zastosowanych scenariuszy testów socjotechnicznych. d) Raport z przeprowadzonych testów, obejmujący wyniki, ocenę reakcji personelu, zgodność postępowania z procedurami SZBI oraz zalecenia. e) Zaświadczenia lub certyfikaty uczestnictwa w szkoleniu. Warunkiem odbioru zamówienia jest przeprowadzenie szkolenia w wymiarze 6 godzin lekcyjnych, realizacja uzgodnionych testów socjotechnicznych oraz przekazanie wymaganej dokumentacji.	

37. Audyt cyberbezpieczeństwa sieci OT/IT/ICS/IIOT

Lp.	Wymagania minimalne	Spełnia wymogi Tak/Nie (wpisać poniżej)
1	Audyt należy przeprowadzić na podstawie uzgodnionego z Zamawiającym zakresu i harmonogramu.	
2	Audyt powinien obejmować analizę dokumentacji, konfiguracji zabezpieczeń oraz czynności weryfikacyjne dotyczące infrastruktury sieciowej.	
3	Identyfikację podatności należy przeprowadzać metodami odpowiednimi do specyfiki badanych środowisk IT lub OT.	
4	W środowiskach OT, ICS i IIoT należy stosować w pierwszej kolejności metody pasywne. Aktywne skanowanie i testy mogące wpłynąć na działanie systemów wymagają odrębnej zgody Zamawiającego.	
5	Czynności audytowe nie mogą powodować nieuzgodnionych zakłóceń w funkcjonowaniu infrastruktury sieciowej i procesów technologicznych.	
6	Audyt ma być realizowany stacjonarnie, z możliwością przeprowadzenia części czynności zdalnie, po uzgodnieniu z Zamawiającym.	
7	Wykonawca zobowiązany jest do zachowania poufności informacji uzyskanych podczas audytu.	
8	Wykonawca zobowiązany jest zapewnić personel posiadający kwalifikacje i doświadczenie odpowiednie do zakresu audytu: Personel wykonujący czynności techniczne posiada wiedzę i doświadczenie w zakresie bezpieczeństwa sieci komputerowych, identyfikacji podatności, konfiguracji zabezpieczeń oraz specyfiki środowisk objętych audytem.	
9	Dokumentacja i odbiór zamówienia Po zakończeniu audytu Wykonawca przekaże Zamawiającemu raport końcowy zawierający: a) Opis zakresu i zastosowanych metod audytu. b) Wyniki oceny bezpieczeństwa infrastruktury sieciowej. c) Wykaz zidentyfikowanych podatności i słabości zabezpieczeń. d) Ocenę ryzyka związanego ze stwierdzonymi słabościami. e) Zalecenia dotyczące działań naprawczych wraz z określeniem priorytetów ich realizacji. f) Podsumowanie wyników audytu. Warunkiem odbioru zamówienia jest przeprowadzenie audytu zgodnie z uzgodnionym zakresem oraz przekazanie Zamawiającemu raportu zawierającego wyniki oceny bezpieczeństwa sieci, zidentyfikowane podatności, ocenę ryzyka i zalecenia dotyczące poprawy bezpieczeństwa.	