Nr sprawy: 48/ZP-Z/2026

Załącznik nr 3 do SWZ

Opis przedmiotu zamówienia
„Podniesienie poziomu cyberbezpieczeństwa infrastruktury wodociągowej w Konstantynowie Łódzkim”

Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (dalej SzOPZ lub OPZ) w zakresie dostawy oraz wdrożenia sprzętu i oprogramowania służącego zabezpieczeniu działania infrastruktury Zamawiającego oraz niezbędnych szkoleń. Wszystkie parametry techniczne określone w niniejszym OPZ określają graniczne (minimalne lub maksymalne - zgodnie z opisem) wymagania stawiane oferowanym urządzeniom i oprogramowaniu, co oznacza, że jeśli Wykonawca zaoferuje przedmioty posiadające więcej funkcji niż wymagane minimum lub w lepszym stopniu, nie zostaną mu przyznane żadne dodatkowe punkty. Wykonawca może zaoferować rozwiązania równoważne spełniające minimum opisane w OPZ.

Ogólny zarys projektu

Celem projektu jest wdrożenie i konfiguracja nowoczesnych systemów zabezpieczeń infrastruktury i danych Zamawiającego. Zamawiający oczekuje dostarczenia systemów informatycznych, uruchomienia (w tym instalacja i parametryzacja), przeprowadzenia instruktażu personelu. Dodatkowym elementem wzmocnienia cyberbezpieczeństwa będą szkolenia dla pracowników i stworzenie dokumentacji SZBI.

Wymagania ogólne

Zamawiający wymaga, by dostarczony sprzęt i oprogramowanie były w wersji aktualnej na dzień jego instalacji.

System musi mieć możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Zadanie 1 - Obszar organizacyjny

1. Opracowanie strategii bezpieczeństwa

Przedmiotem zamówienia jest opracowanie Strategii Cyberbezpieczeństwa dla Zamawiającego, uwzględniającej specyfikę działalności przedsiębiorstwa wodociągowo-kanalizacyjnego, w szczególności bezpieczeństwo infrastruktury informatycznej (IT), systemów technologii operacyjnych (OT) oraz systemów sterowania przemysłowego (SCADA). Strategia ma określać główne cele, kierunki rozwoju oraz priorytety działań w zakresie cyberbezpieczeństwa, stanowiąc podstawę do dalszego opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Systemu Zarządzania Ciągłością Działania (SZCD).

Zakres

Wykonawca zobowiązany jest do:

- Przeprowadzenia ogólnej analizy aktualnego stanu cyberbezpieczeństwa Zamawiającego na podstawie udostępnionej dokumentacji oraz informacji uzyskanych od przedstawicieli Zamawiającego
- Identyfikacji kluczowych obszarów działalności i zasobów IT/OT wymagających ochrony
- Określenia głównych zagrożeń i obszarów ryzyka związanych z cyberbezpieczeństwem oraz ciągłością świadczenia usług wodociągowo-kanalizacyjnych
- Zdefiniowania celów strategicznych w obszarze cyberbezpieczeństwa
- Określenia kierunków rozwoju zabezpieczeń organizacyjnych i technicznych, w tym zarządzania dostępem, monitorowania bezpieczeństwa, zarządzania podatnościami, ochrony systemów IT/OT oraz reagowania na incydenty
- Określenia założeń dotyczących zarządzania bezpieczeństwem informacji i ciągłością działania, stanowiących podstawę do późniejszego opracowania SZBI i SZCD
- Przygotowania planu działań (roadmapy) zawierającego priorytety, rekomendowane przedsięwzięcia oraz orientacyjny harmonogram ich realizacji

Strategia powinna:

- Uwzględniać wymagania wynikające z obowiązujących przepisów dotyczących cyberbezpieczeństwa, w szczególności ustawy o krajowym systemie cyberbezpieczeństwa, w zakresie mającym zastosowanie do Zamawiającego
- Uwzględniać dobre praktyki wynikające z norm ISO/IEC 27001, ISO 22301 oraz IEC 62443, w zakresie odpowiednim do charakteru działalności Zamawiającego
- Być dostosowana do specyfiki infrastruktury wodociągowo-kanalizacyjnej i środowisk IT/OT
- Zawierać realne i możliwe do wdrożenia rekomendacje, uwzględniające możliwości organizacyjne i finansowe Zamawiającego

- Stanowić dokument kierunkowy, umożliwiający zaplanowanie kolejnych etapów podnoszenia poziomu cyberbezpieczeństwa

Wykonawca zobowiązany jest do przekazania:

- Dokumentu „Strategia Cyberbezpieczeństwa".
- Planu działań (roadmapy) z określeniem priorytetów i orientacyjnych terminów realizacji.
- Zestawienia najważniejszych rekomendacji organizacyjnych i technicznych.
- Dokumentacja musi zostać przekazana w formacie edytowalnym DOCX lub XLSX, odpowiednio do rodzaju dokumentu, oraz PDF.

Podstawą odbioru będzie przekazanie kompletnej Strategii Cyberbezpieczeństwa wraz z planem działań, uwzględnienie specyfiki działalności Zamawiającego oraz omówienie rekomendacji z przedstawicielami Zamawiającego.

Strategia Cyberbezpieczeństwa ma stanowić dokument nadrzędny i kierunkowy dla dalszych prac związanych z opracowaniem i wdrożeniem SZBI oraz SZCD.

2. Ustanowienie Systemu Zarządzania Bezpieczeństwem informacji SZBI

W ramach ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zostanie zaprojektowany system zarządzania bezpieczeństwem informacji wraz z umocowaniem w organizacji Zamawiającego, przygotowana i wdrożona kompleksowa dokumentacja SZBI, obejmująca polityki i procedury bezpieczeństwa informacji, w tym w szczególności polityka zarządzania kontami i dostępami, polityka haseł, polityka zarządzania podatnościami oraz polityka bezpiecznej konfiguracji systemów, jak również zasady zarządzania ryzykiem zgodne z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz normy ISO/IEC 27001, z uwzględnieniem dobrych praktyk w zakresie AI.

System zostanie dostosowany do specyfiki działalności Zamawiającego, obejmując ochronę danych związanych m.in. z infrastrukturą wodociągową, danymi odbiorców oraz wrażliwymi informacjami dot. sieci i urządzeń.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) musi uwzględniać:

- specyfikę działalności Zamawiającego,
- wymagania ustawy o KSC,
- proporcjonalnych środków organizacyjnych i technicznych,
- aktualnych uwarunkowań technologicznych i organizacyjnych.

W wyniku realizacji zamówienia nastąpi:

- Stworzenie procesu analizy ryzyka
- Przeprowadzenie analizy ryzyka
- Stworzenie procesu zarządzania podatnościami
- Zdefiniowanie i wdrożenie procesu zarządzania dostawcami
- Wdrożenie procesu inwentaryzacji
- Zdefiniowanie polityki zarządzania kontami i dostępami oraz polityki haseł
- Zdefiniowanie domyślnej bezpiecznej konfiguracji i wprowadzenie rejestru zmian
- Zdefiniowanie i wdrożenie procesu aktualizacji SW/HW

- Plan reagowania na incydenty, wraz z macierzą komunikacji i przypisaniem ról oraz odpowiedzialności

Opracowana dokumentacja SZBI będzie pokrywała przynajmniej poniższe obszary:

- Bezpieczeństwo informacji
- Zarządzanie ryzykiem ICT
- Analiza ryzyka i ocena ryzyka
- Plany postępowania z ryzykiem
- Dostępy i zarządzanie tożsamością
- Zarządzanie incydentami bezpieczeństwa ICT
- Zarządzanie ciągłością działania (BCP)
- Kontrolę dostępu fizycznego i środowiskowego
- Kryptografię
- Zarządzanie dostawcami ICT
- Zarządzanie zasobami informacyjnymi
- Archiwizację i backup
- Usuwania i niszczenia danych
- Monitorowania i logowania zdarzeń
- Zarządzanie oprogramowaniem
- Klasyfikację i etykietowanie informacji
- Zarządzanie bezpieczeństwem w projektach
- Segregację obowiązków
- Przeglądy i testy planów ciągłości działania
- Stosowanie MFA
- Zarządzanie nieautoryzowanymi próbami dostępu
- Zarządzania aktualizacjami bezpieczeństwa
- Dokumentację wersjonowania procedur
- Ochronę sieci
- Kontrolę uprawnień
- Zarządzanie konfiguracją systemów ICT
- Retencję danych
- Zarządzanie dostawcami: oceny i walidacja dostawców pod kątem bezpieczeństwa, określanie krytyczności poddostawców
- Testy penetracyjne
- Bezpieczne korzystanie z narzędzi AI

i musi zostać opracowana zgodnie z normą ISO 27001.

W ramach zadania zostaną również opracowane wzorce dokumentów wspierających:

- Plan zarządzania kryzysowego
- Rejestr incydentów bezpieczeństwa ICT
- Rejestr dostawców ICT
- Ankieta oceny zgodności dostawców ICT

- Propozycje rekomendowanych zapisów do umówi z dostawcami ICT
- Ankieta weryfikująca dla dostawców ICT

3. Opracowanie, planów ciągłości działania (BCP) i odtwarzania po awarii (DRP)

W ramach zadania powstaną dedykowane plany ciągłości działania (BCP) oraz plany odtwarzania po awarii (DRP), uwzględniające kluczowe procesy związane z dostawą wody, jako usługą krytyczną dla mieszkańców. System Zarządzania Ciągłością Działania będzie obejmował scenariusze dotyczące m.in. awarii pompowni, uszkodzeń sieci, przerw w dostawie energii, cyberataków na systemy SCADA oraz incydentów wpływających na jakość lub dostępność wody. Wdrożone rozwiązania ma zapewnić szybkie i skuteczne przywracanie ciągłości dostaw w sytuacji zagrożenia.

W wyniku realizacji zamówienia nastąpi:

- Opracowanie planów ciągłości działania, tworzenia i testowania kopii zapasowych oraz ich odtwarzania
- Opracowanie planu reagowania na incydenty oraz macierzy komunikacji

Plan Ciągłości Działania powinien określać co najmniej:

- zasady i przesłanki uruchomienia planu;
- role i odpowiedzialności;
- sposób eskalacji i komunikacji;
- procedury działania w sytuacji awaryjnej;
- minimalny poziom działania krytycznych usług;
- zasady działania w trybie zastępczym;
- plan powrotu do normalnego trybu pracy.

Plan Odtwarzania po Awarii powinien zawierać co najmniej:

- kolejność odtwarzania systemów;
- zależności techniczne pomiędzy systemami;
- procedury odtworzenia infrastruktury, systemów, aplikacji i danych;
- procedury odtworzenia z kopii zapasowych;
- zasady weryfikacji integralności i poprawności odtworzonych systemów;
- procedury postępowania w przypadku niepowodzenia odtworzenia;
- zasady bezpiecznego przywrócenia systemów do eksploatacji;
- zasady komunikacji zewnętrznej i wewnętrznej w przypadku awarii (w tym komunikacja z mieszkańcami, mediami, NASK, itp.).

Dla krytycznych systemów Wykonawca opracuje karty lub instrukcje odtwarzania zawierające co najmniej RTO, RPO, zależności, lokalizację kopii zapasowych, kolejność czynności oraz sposób weryfikacji odtworzenia.

BCP i DRP powinny uwzględniać co najmniej:

- awarię serwera, środowiska wirtualizacyjnego lub pamięci masowej;

- awarię infrastruktury sieciowej;
- utratę łącza Internet/WAN;
- awarię usług katalogowych i infrastrukturalnych;
- atak ransomware lub inny cyberatak;
- awarię zasilania;
- utratę dostępu do serwerowni;
- niedostępność kluczowego personelu lub dostawcy zewnętrznego;

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego i wdrażanej jednostki w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami na etapie deklaracji stosowania oraz wszelkich innych informacji uzyskanych przez Wykonawcę w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Usługi dotyczące czynności wdrażających dokumentację zostanie uznana za wykonaną po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI i podpisaniu protokołu odbioru przez Zamawiającego.

3. Testy bezpieczeństwa infrastruktury sieciowej IT/OT

Weryfikacja bezpieczeństwa infrastruktury sieciowej w obszarach IT poprzez przeprowadzenie specjalistycznych testów penetracyjnych

Testy sieci zewnętrznej

- Skanowanie i testy podatności na zewnętrznych adresach IP
- Testy penetracyjne na aktywnych adresach IP (w tym serwery, urządzenia sieciowe, usługi zdalnego dostępu)
- Testy bezpieczeństwa usług zdalnych
- Testy bezpieczeństwa stron internetowych i aplikacji webowych dostępnych z Internetu
- Próby logowania przy użyciu słabych haseł lub błędnie skonfigurowanych kluczy SSH
- Eksploatacja podatności w oprogramowaniu serwerowym
- Próby obejścia mechanizmów uwierzytelniania i autoryzacji
- Próby uzyskania dostępu do danych przez błędne konfiguracje
- Eksploatacja podatności w systemach zarządzania bazami danych
- Ataki na Zewnętrzne Usługi Poczty Elektronicznej
- Analiza konfiguracji serwerów pocztowych
- Testy zabezpieczeń protokołów pocztowych
- Ataki na Zewnętrzne Usługi Plikowe
- Weryfikacja dostępów do danych przechowywanych na zewnętrznych serwerach plikowych
- Testy zabezpieczeń udostępnionych plików i katalogów
- Próby eksfiltracji danych wrażliwych z niewłaściwie skonfigurowanych dostępów
- Ataki na Zewnętrzne Usługi DNS
- Analiza konfiguracji serwerów DNS i próby przejęcia kontroli nad domenami

- Testy podatności na ataki typu DNS spoofing czy cache poisoning
- Ataki na Zewnętrzne Usługi VPN
- Weryfikacja zabezpieczeń konfiguracji VPN
- Eksploatacja podatności w oprogramowaniu VPN
- Próby dostania się do sieci wewnętrznej

Testy sieci wewnętrznej

Ataki sieciowe (na routery, przełączniki, AP, drukarki, kamery IP, telefony VoIP i inne urządzenia znajdujące się w sieci):

- Atak na domyślne loginy w interfejsach zarządzania urządzeniami
- Przechwycenie lub modyfikacja konfiguracji urządzeń poprzez protokół SNMP
- Zdalne wykonanie kodu poprzez podatności w niezałatanych wersjach oprogramowania sprzętowego
- Próby wykorzystania błędów konfiguracji VLAN na switchu
- Testy nadużycia protokołu UPnP do otwarcia portów lub przekierowania ruchu na routerze
- Telnet/SSH Brute-Force
- Camera RTSP Exploit
- Kradzież plików konfiguracyjnych urządzeń bez uwierzytelnienia

Zatruwanie ruchu sieciowego, przynajmniej w poniższym zakresie:

- DNS Cache Poisoning
- DHCP Spoofing/Poisoning
- NDP (Neighbor Discovery Protocol) Poisoning
- mDNS Poisoning
- WINS Poisoning
- ICMP Redirect Poisoning
- Proxy ARP Poisoning
- RIP/OSPF Routing Poisoning
- SSDP/UPnP Poisoning

Ataki na bazy danych i aplikacje wewnętrzne:

- SQL Server Links Exploitation
- MSSQL xp_cmdshell Abuse

Weryfikacja architektury sieciowej i mechanizmów obronnych:

- Testowanie skuteczności izolacji stref sieciowych oraz weryfikacja filtracji ruchu wychodzącego pod kątem możliwości ustanowienia kanałów C2
- Próby aktywnego omijania, wyłączania lub manipulacji lokalnymi agentami systemów antywirusowych oraz klas EDR na przejętych stacjach roboczych

Raport z testów powinien zawierać:

1. Podsumowanie dla Zarządu
   - Podsumowanie wykonanych prac w sposób nietechniczny

- Opis najistotniejszych podatności (krytycznych i wysokich) w sposób nietechniczny

2. Szczegółowy raport techniczny
   - Zakres testów
   - Podsumowanie testów bezpieczeństwa
   - Lista wykrytych podatności
   - Szczegółowy opis podatności
   - Kategoria krytyczności/klasyfikacji podatności
   - Pewność identyfikacji
   - Szczegółowy opis wykrytej podatności
   - Potencjalne metody wykorzystania podatności w oparciu o framework MITRE ATT&CK oraz dowodów w postaci zrzutów ekranu, logów
   - Rekomendacje w celu usunięcia podatności, naprawy wykrytych problemów
   - Ogólne sugerowane zalecenia/rekomendacje dotyczące poprawy bezpieczeństwa sieci

Testy powinny być wykonane wg następujących standardów:

a) NIST SP800-115
b) PTES (Penetration Testing Execution Standard)

Testy sieci OT

Przedmiotem zamówienia jest wykonanie usługi polegającej na przeprowadzeniu pasywnej analizy cyberbezpieczeństwa infrastruktury OT Zamawiającego, w szczególności sieci automatyki przemysłowej, wraz z dostarczeniem na czas realizacji usługi niezbędnego sprzętu, oprogramowania, licencji, konfiguracji, wsparcia eksperckiego oraz opracowaniem raportu końcowego.

Celem analizy są:

- inwentaryzacja urządzeń i zasobów komunikujących się w ramach infrastruktury OT
- identyfikacja topologii komunikacyjnej oraz relacji pomiędzy urządzeniami w warstwie L2 i L3
- identyfikacja protokołów wykorzystywanych w sieci OT, w tym protokołów przemysłowych oraz protokołów pomocniczych/IT obecnych w tej sieci
- wskazanie dominujących typów ruchu oraz potencjalnych źródeł przeciążenia lub zakłóceń
- wykrycie anomalii, zdarzeń bezpieczeństwa, niepożądanych połączeń, nietypowych zapytań, zmian charakterystyki ruchu oraz innych obserwacji istotnych dla bezpieczeństwa sieci OT
- identyfikacja urządzeń posiadających znane podatności, o ile możliwe będzie ich powiązanie z zaobserwowanymi danymi technicznymi, takimi jak producent, typ, wersja oprogramowania lub identyfikator CPE
- przygotowanie rekomendacji dotyczących mitygacji ryzyka, segmentacji, ograniczenia niepożądanej komunikacji, hardeningu urządzeń i praktyk typu defense in depth
- opracowanie raportu końcowego oraz załączników technicznych umożliwiających Zamawiającemu dalsze prace projektowe i decyzyjne

Analiza powinna zostać przeprowadzona w sposób nieinwazyjny i bezpieczny dla środowiska produkcyjnego OT. Podstawowym trybem realizacji jest pasywne monitorowanie kopii ruchu sieciowego, pozyskanej z portów lustrzanych SPAN/RSPAN/ERSPAN, TAP lub innej metody zaakceptowanej przez Zamawiającego. Wykonawca nie może wykonywać aktywnego skanowania, testów penetracyjnych, prób eksploatacji podatności, modyfikacji konfiguracji urządzeń automatyki ani generowania ruchu do urządzeń OT bez uprzedniej, jednoznacznej zgody Zamawiającego wyrażonej w trybie roboczym lub pisemnym.

Wymagania dotyczące sposobu realizacji prac

Bezpieczeństwo i nieinwazyjność

- Prace muszą być prowadzone z zachowaniem ciągłości działania procesów technologicznych Zamawiającego.
- Domyślnym sposobem podłączenia jest odbiór kopii ruchu z portu lustrzanego lub TAP. Rozwiązanie Wykonawcy nie może wymagać modyfikacji konfiguracji sterowników PLC, RTU, HMI, SCADA ani urządzeń wykonawczych.
- Wykonawca nie może samodzielnie inicjować ruchu testowego do urządzeń OT, wykonywać aktywnego skanowania, prób logowania, testów haseł, eksploatacji podatności lub zmian konfiguracji urządzeń, chyba że Zamawiający dopuści taki scenariusz na piśmie lub w uzgodnionym protokole roboczym.
- Wykonawca jest zobowiązany niezwłocznie zgłaszać Zamawiającemu wszelkie zaobserwowane zdarzenia mogące wskazywać na aktywny incydent bezpieczeństwa, zakłócenie pracy sieci, ryzyko utraty dostępności lub istotną podatność urządzeń krytycznych.
- W przypadku wykrycia okoliczności mogących wpłynąć na bezpieczeństwo procesu technologicznego Wykonawca ma obowiązek przerwać działania w danym zakresie i uzgodnić dalszy tryb prac z Zamawiającym.

Minimalne wymagania dla narzędzia/systemu analitycznego

- Możliwość analizy kopii ruchu sieciowego bez ingerencji w urządzenia OT i bez konieczności instalowania agentów na sterownikach, panelach HMI, stacjach operatorskich lub serwerach SCADA.
- Możliwość pracy w środowisku automatyki przemysłowej oraz analizy protokołów przemysłowych i pomocniczych występujących w sieciach OT. Wykonawca powinien wskazać listę obsługiwanych protokołów istotnych dla środowiska Zamawiającego.
- Identyfikacja urządzeń fizycznych i logicznych na podstawie obserwowanego ruchu, z przypisaniem co najmniej adresów MAC/IP, producenta, typu urządzenia, nazwy lub wersji oprogramowania, jeżeli możliwe jest ich ustalenie z ruchu sieciowego.
- Prezentacja połączeń między urządzeniami, przepływów komunikacyjnych oraz wizualizacji warstw L2 i L3 lub równoważnej prezentacji relacji komunikacyjnych.

- Identyfikacja protokołów, podsieci, udziałów procentowych ruchu, parametrów takich jak pps, średnia długość pakietu, wolumen ruchu, top talkers oraz ruch o charakterze burstowym.
- Wykrywanie zdarzeń bezpieczeństwa, anomalii ruchu, nowych lub znikających urządzeń i połączeń, nietypowych zapytań DNS, zmian TTL, skanowania sieci, zmian profilu ruchu oraz innych obserwacji wskazujących na ryzyko cyberbezpieczeństwa.
- Możliwość powiązania wykrytych urządzeń i wersji oprogramowania ze znanymi podatnościami, np. na podstawie CPE/CVE lub równoważnych baz, z określeniem poziomu ryzyka i rekomendacji mitygacji.
- Możliwość eksportu wyników analizy, list urządzeń, protokołów, podsieci, połączeń, podatności oraz wybranych danych PCAP dla wskazanych przepływów lub przedziałów czasu.
- Możliwość przygotowania raportu zarządczego i technicznego, zawierającego opis ryzyka, dowody obserwacji, priorytety rekomendacji i załączniki techniczne.

Wykonawca zobowiązuje się do:

- dostarczenia wszystkich komponentów, licencji, oprogramowania, sensorów, serwera lub zasobów koniecznych do wykonania usługi
- przeprowadzenia instalacji, konfiguracji i weryfikacji poprawności działania rozwiązania testowego
- realizacji analizy zgodnie z zasadą minimalnej ingerencji w środowisko OT
- prowadzenia prac przez osoby posiadające doświadczenie w zakresie sieci przemysłowych, cyberbezpieczeństwa OT oraz analizy ruchu sieciowego
- bieżącego informowanie Zamawiającego o istotnych ryzykach, zdarzeniach, utrudnieniach i ograniczeniach analizy
- opracowania raportu końcowego i załączników w języku polskim
- zachowania poufności wszystkich informacji uzyskanych w toku realizacji zamówienia
- usunięcia lub zwrotu danych i nośników zgodnie z zasadami określonymi przez Zamawiającego po zakończeniu projektu, z zastrzeżeniem obowiązków wynikających z prawa i umowy

Raport z testów powinien zawierać:

Lp.	Obszar	Minimalna zawartość
1	Streszczenie zarządcze	Najważniejsze wnioski, poziom ryzyka, lista najpilniejszych działań oraz ogólna ocena stanu widocznej części infrastruktury OT.
2	Zakres i metodyka	Opis lokalizacji, punktów pomiarowych, okresu analizy, sposobu podłączenia, ograniczeń i założeń.
3	Inwentaryzacja	Lista urządzeń fizycznych i logicznych, adresów MAC/IP, producentów, wersji oprogramowania, ról, podsieci i protokołów, o ile możliwe do ustalenia.

4	Topologia i komunikacja	Wizualizacja lub opis relacji L2/L3, połączeń między urządzeniami, top talkers, kierunków komunikacji i zależności.
5	Analiza statystyczna ruchu	Pps, wolumeny, średnia długość pakietu, podział protokołów, ruch burstowy, ruch kamer lub innych źródeł dużego wolumenu, jeżeli wystąpi.
6	Zdarzenia, zagrożenia i anomalie	Opis wykrytych zdarzeń, ich wpływu na bezpieczeństwo, osi czasu, urządzeń źródłowych/docelowych oraz dowodów.
7	Podatności	Lista znanych podatności przypisanych do urządzeń, poziom krytyczności, potencjalny wpływ i rekomendowana mitygacja.
8	Rekomendacje	Rekomendacje techniczne i organizacyjne, w tym priorytetyzacja działań: krytyczne, wysokie, średnie, niskie oraz quick wins.
9	Ograniczenia analizy	Opis braku widoczności części ruchu, ograniczeń wynikających z braku danych o wersjach, niemożności wykonania symulacji lub innych czynników wpływających na kompletność wniosków.
10	Załączniki techniczne	Listy urządzeń, protokołów, podsieci, połączeń, podatności, wybrane PCAP.

Format przekazania wyników

- Raport końcowy powinien zostać przekazany w formacie PDF oraz edytowalnym DOCX lub równoważnym, chyba że Zamawiający wskaże inaczej.
- Załączniki techniczne powinny zostać przekazane w formacie CSV/XLSX/PDF lub innym uzgodnionym formacie umożliwiającym dalszą analizę.

4. Wykonanie usługi przeglądu bezpieczeństwa

Wykonawca przeprowadzi audyt zgodności organizacji Zamawiającego z KRI/uoKSC.

ZADANIE 2 - Obszar kompetencyjny

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego dla wszystkich pracowników dotyczącego bezpieczeństwa informacji, budującego świadomość cyberzagrożeń, wskazującego skutki naruszeń zasad bezpieczeństwa informacji oraz kwestie prawne związane z ochroną danych osobowych i sposobów ochrony. Celem szkolenia jest podniesienie świadomości uczestników w zakresie bezpieczeństwa informacji, umożliwiając im lepsze zrozumienie zagrożeń, skutków naruszeń i efektywne stosowanie środków bezpieczeństwa w codziennej pracy. Zamawiający zapewni salę szkoleniową wyposażoną w ekran lub rzutnik.

Wymagania:

1. Szkolenia muszą odbywać się w godzinach pracy Zamawiającego.

2. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia, do akceptacji Zamawiającego.

Część I – Szkolenie specjalistyczne dla kadry - szkolenia z zakresu cyberbezpieczeństwa kadry kierowniczej istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS

Przedmiotem zamówienia jest przeprowadzenie szkolenia dla kadry kierowniczej z zakresu zarządzania polityką bezpieczeństwa informacji, reagowania na incydenty i podejmowania decyzji w sytuacjach kryzysowych.
Uczestnicy poznają zasady zgodne z SZBI:

- zarządzanie ryzykiem
- klasyfikację informacji
- nadawanie uprawnień
- monitorowanie incydentów w systemach sterujących pracą infrastruktury wodociągowej.

Szkolenia zapewnią jednolite stosowanie procedur bezpieczeństwa w całej organizacji oraz obejmą dodatkowe obszary cyberbezpieczeństwa w tym minimalnie:

- Rodzaje i koszty cyberataków
- Konsekwencje ataków
- Wpływ sytuacji geopolitycznej i gospodarczej na cyberbezpieczeństwo
- Wpływ sztucznej inteligencji (AI) na krajobraz cyber
- Jak rozpoznawać zagrożenia
- Jak chronić się przed atakami, szczególnie w dobie AI
- Rola kadry kierowniczej w budowaniu odporności organizacji
- Bezpieczne zachowania i zgłaszania incydentów
- System Zarządzania Bezpieczeństwem Informacji – czym jest
- Analiza ryzyka jako podstawa działań prewencyjnych i odpowiedzialność zarządu
- Procedury reagowania w kryzysie
- Plan ciągłości działania
- Różne płaszczyzny bezpieczeństwa
- Minimalna higiena bezpieczeństwa IT
- Bezpieczeństwo w firmie i w domu
- Komunikacja kryzysowa (wewnętrzna i zewnętrzna)
- Pierwsze kroki po identyfikacji incydentu

Wykonawca zapewni przynajmniej jeden termin szkolenia stacjonarnego (czas trwania min. 5h). Zamawiający zastrzega sobie prawo do zmiany formy szkolenia ze szkolenia stacjonarnego na online według własnego uznania.

Część II - Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony

Wykonawca przeprowadzi cykl szkoleń dla pracowników. Podstawowe szkolenia z cyberbezpieczeństwa mają na celu podniesienie świadomości pracowników w zakresie typowych zagrożeń cyfrowych oraz sposobów ich unikania.
Obejmą zasady bezpiecznego korzystania z systemów obsługujących infrastrukturę wodociągową, rozpoznawanie phishingu, ochronę danych oraz właściwe reagowanie na podejrzane komunikaty, wpływające na ciągłość dostaw wody.

1. Szkolenie stacjonarne z trenerem na żywo w siedzibie Zamawiającego lub innej lokalizacji wskazanej przez Zamawiającego dla 63 pracowników Zamawiającego.
   Wykonawca przeprowadzi szkolenie dla 2 grup.
2. Zamawiający zastrzega sobie prawo do zmiany formy szkolenia (jednej lub większej ilości grup) ze szkolenia stacjonarnego na online według własnego uznania.
3. Szkolenie jednej grupy powinno trwać przynajmniej 3 godziny i musi obejmować co najmniej następującą tematykę:

Bezpieczeństwo fizyczne

- Bezpieczeństwo dostępu do obiektu - tailgating
- Bezpieczeństwo fizycznych dokumentów
- Dostęp fizyczny do sprzętu w firmie i zewnętrzne nośniki pamięci

Cyberbezpieczeństwo

- Phishing i Spear phishing
- Ransomware
- DDoS
- Vishing
- Bezpieczna instalacja oprogramowania
- Bezpieczeństwo skrzynki mailowej
- Wieloskładnikowe uwierzytelnianie
- Bezpieczeństwo haseł
- Bezpieczeństwo płatności online

Bezpieczeństwo danych firmowych

- Rozmowy o pracy w miejscach publicznych
- Udostępnianie danych na zewnątrz
- Szyfrowanie danych
- Makra
- Niszczenie i usuwanie danych
- Użytkowanie urządzeń prywatnych
- Korzystanie z publicznych sieci wifi

Bezpieczna praca z przeglądarką

- HTTPS
- Certyfikaty SSL
- Ciasteczka
- Wtyczki – dobre praktyki

Bezpieczeństwo psychiczne w sieci:

- Bezpieczne korzystanie z mediów społecznościowych
- Wykorzystanie sztucznej inteligencji w socjotechnikach
- Fake Newsy i dezinformacja
- Deepfake
- Stalking i Cyberstalking

Wykonawca dostarczy dla maksymalnie 63 pracowników dostęp do platformy e-learningowej ze szkoleniem z cyberbezpieczeństwa na okres 12 m-cy, w tym przynajmniej jedną aktualizację treści rocznie.
Platforma musi mieć funkcję generowania raportów z postępami pracowników, zawierać testy sprawdzające oraz możliwość wygenerowania certyfikatu po zaliczeniu testów.

Część III – Szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS

Kadra kierownicza i informatycy zostaną przygotowani do obsługi i rozwijania środków bezpieczeństwa wdrażanych w ramach projektu.
Zajęcia obejmą ochronę sieci, zabezpieczenia systemów monitorujących bezpieczeństwo sieci, ochronę urządzeń sterowania oraz metody wykrywania prób nieautoryzowanego dostępu.
Szkolenie specjalistyczne dla kadry IT i administratorów systemów teleinformatycznych, dotyczące wdrożonych i planowanych środków ochrony, konfiguracji zabezpieczeń, obsługi narzędzi monitorujących i systemów IDS/IPS.
1. Szkolenie dla kadry i informatyków online (min. 3h) – 1 grupa.
2. Szkolenie specjalistyczne dla kadry IT i administratorów online (min. 3h) – 1 grupa.

ZADANIE 3 - Obszar techniczny IT
Część I – Usługa segmentacji sieci IT/OT/ICS/IIoT
Wdrożenie właściwej segmentacji i konfiguracji na styku sieci oraz separacji i segmentacji sieci IT/OT

Sieć biurowa:

Wykonawca wdroży segmentację (VLAN) z dedykowaną podsiecią, co najmniej dla: stanowisk użytkowników, serwerów, zarządzania urządzeniami, kopii zapasowych, drukarek

oraz gości. Ruch między segmentami będzie domyślnie zablokowany i dopuszczony tylko tam, gdzie wynika to z potrzeb pracy, na podstawie listy dozwolonych połączeń uzgodnionej z Zamawiającym. Segment kopii zapasowych i segment zarządzania będą dostępne wyłącznie ze stanowisk administratorów, a sieć dla gości wyłącznie do Internetu.

W ramach zadania Wykonawca zarezerwuje pulę adresów IP dla, usług DHCP i DNS oraz dokona rekonfiguracji aktywnych urządzeń sieciowych LAN (sieć przewodowa) oraz WLAN, sieć bezprzewodowa, a zdezaktywuje wszystkie nieużywane funkcje. W rezultacie sieć uzyska pełną separację oraz agregację, ograniczającą skutki ataku DI jednej podsieci oraz uniemożliwi propagację ataku do innych segmentów sieci. Dodatkowo ruch między vlanami oraz wewnątrz VLAN'ów zostanie ograniczony w oparciu o listy kontroli dostępu, które będą definiowały zasady komunikacji między urządzeniami.

Wdrożenie właściwej konfiguracji na styku sieci

Styki sieci technologicznej (OT) z siecią biurową (IT) i z Internetem są pierwszą linią obrony instalacji. Dlatego powinny przepuszczać wyłącznie ruch znany, potrzebny i opisany. Sieć OT nie może mieć bezpośredniego połączenia z Internetem.

Wykonawca zinwentaryzuje wszystkie połączenia sieci OT z innymi sieciami, w tym łącza serwisowe, modemy GSM/LTE, łącza dostawców i połączenia urządzeń z chmurą producentów. Następnie przejrzy reguły firewalli, przekierowania portów i translacje adresów na granicach OT/IT i IT/Internet. Reguły zbędne, zbyt szerokie lub o nieznanym przeznaczeniu zostaną usunięte albo zawężone. Każda pozostawiona reguła otrzyma opis obejmujący cel, właściciela, źródło, miejsce docelowe, protokół i port. Zmiany będą wprowadzane w oknach serwisowych uzgodnionych z Zamawiającym, po ocenie wpływu na proces technologiczny i z przygotowanym planem wycofania.

Sieć OT zostanie oddzielona od sieci IT przemysłową strefą zdemilitaryzowaną (IDMZ), zgodnie z modelem stref i kanałów komunikacyjnych IEC 62443. Ruch nie będzie przechodził bezpośrednio między IT a OT. Wymiana danych (np. historia, raporty, aktualizacje, sygnatury antywirusowe) będzie odbywać się przez serwery pośredniczące w IDMZ, a tam, gdzie to uzasadnione, przez połączenia jednokierunkowe. Bezpośredni dostęp z Internetu i z sieci IT do urządzeń OT zostanie zablokowany. Dotyczy to w szczególności sterowników, HMI, serwerów SCADA, pulpitu zdalnego i interfejsów zarządzania.

Zdalny dostęp pracowników i firm serwisowych będzie możliwy wyłącznie przez szyfrowane połączenie VPN z uwierzytelnianiem wieloskładnikowym, zakończone w IDMZ, a dalej przez serwer przesiadkowy (jump host). Dostęp serwisowy będzie:

- włączany na żądanie, po akceptacji Zamawiającego,
- ograniczony w czasie i do wskazanych urządzeń,
- realizowany z indywidualnych kont, bez kont współdzielonych,
- rejestrowany, a sesje nagrywane.

Niezatwierdzone narzędzia zdalnego dostępu i modemy zostaną usunięte lub zablokowane.

Na styku z Internetem zostaną uruchomione mechanizmy ochrony przed włamaniami, złośliwym oprogramowaniem i niebezpiecznymi stronami. Na granicy IT/OT zostanie zastosowany firewall rozpoznający protokoły przemysłowe używane przez Zamawiającego (np. Modbus TCP, S7, IEC 60870-5-104, IEC 61850, DNP3, OPC UA), z możliwością ograniczenia komunikacji do dozwolonych funkcji, np. zablokowania zapisu i zmiany programu sterownika z sieci IT.
Ruch w sieci OT będzie monitorowany pasywnie, na kopii ruchu (SPAN/TAP), z wykrywaniem anomalii i nowych urządzeń. Mechanizmy blokujące w strefie OT zostaną najpierw uruchomione w trybie obserwacji, a w tryb blokowania przełączone dopiero po akceptacji Zamawiającego. Awaria lub błędna konfiguracja zabezpieczeń nie może zatrzymać procesu technologicznego. Zachowanie urządzeń w razie awarii zostanie uzgodnione z Zamawiającym.
Zdarzenia z urządzeń granicznych, VPN, serwera przesiadkowego i monitoringu OT będą rejestrowane ze zsynchronizowanym czasem z wewnętrznego źródła.
Jeżeli obecne urządzenia nie pozwalają spełnić tych wymagań, Wykonawca wskaże to przed rozpoczęciem wdrożenia i zaproponuje rozwiązanie. Wykonawca przekaże schemat stref i kanałów, macierz dozwolonych przepływów oraz procedurę udzielania dostępu zdalnego.

System urządzeń klasy UTM złożony z dwóch urządzeń pracujących jako HA
Wymagania Ogólne

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym.
3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall ’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
4. System musi wspierać IPv4 oraz IPv6 w zakresie:
   - Firewall.
   - Ochrony w warstwie aplikacji.
   - Protokołów routingu dynamicznego.
5. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów

prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

6. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję UTM musi dysponować minimum:
   8x 1000BASE-T Gigabit Ethernet (10/100/1000 Mbps)
   2x SFP+ 10Gbps Ethernet.
2. System UTM musi posiadać wbudowany port zarządzania 1000BASE-T RJ45, port konsoli RJ45 i/lub port USB Type-C umożliwiające podłączenie się do urządzenia.
3. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa minimum 250 tys. jednoczesnych połączeń.
2. Minimalna liczba obsługiwanych równocześnie połączeń VPN - 280.
3. Przepustowość Stateful Firewall: nie mniej niż 14 Gbps dla pakietów 1500B.
4. Wydajność szyfrowania IPSec VPN dla pakietów 1024B nie mniej niż 9 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami IPS dla pakietów 1024B - minimum 8 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: FW, Antywirus, IPS dla pakietów 1024B - minimum 8 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej TLS – minimum 1.4 Gbps.

Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed atakami - Intrusion Prevention System.

5. Kontrola stron WWW.
6. Analiza ruchu szyfrowanego TLS.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenie VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów.
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla określonych VLAN.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje.
3. Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej adresy URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS.
3. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
4. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
5. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP v3.
5. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
6. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Serwisy i licencje

Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Obrona przed zagrożeniami IPS, ochrona Malware, Kontrola Aplikacji, Web Filtering na okres min. 12 miesięcy,
- Serwis Next Business Day dla UTM na min. 12 m-ce,
- Licencje SSLVPN dla co najmniej 20 użytkowników na min. 12 m-cy.
- Licecnja Virtual Appliance, umożliwiająca scentralizowane zarządzanie minimalnie 3 urządzeniami UTM. Licencja pozwala na konfigurację maszyny wirtualnej w oparciu o środowisko HyperV, VMWare, Cloud.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wdrożenie narzędzi do identyfikacji podatności

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz uruchomienie narzędzia do automatycznego wykrywania podatności bezpieczeństwa, błędów konfiguracji oraz znanych zagrożeń występujących w infrastrukturze informatycznej Zamawiającego.
Rozwiązanie będzie wykorzystywane w przedsiębiorstwie wodociągowo-kanalizacyjnym do identyfikowania podatności systemów IT, serwerów, urządzeń sieciowych, aplikacji internetowych, interfejsów API oraz usług wykorzystywanych do obsługi procesów technologicznych.
System musi umożliwiać prowadzenie cyklicznych oraz doraźnych testów bezpieczeństwa, przy zachowaniu kontroli nad intensywnością i zakresem skanowania, w szczególności w środowiskach powiązanych z infrastrukturą technologii operacyjnych (OT).

Minimalne wymagania techniczne i funkcjonalne

Oferowane rozwiązanie musi spełniać następujące wymagania:

1. Umożliwiać automatyczną identyfikację znanych podatności bezpieczeństwa, w tym podatności oznaczonych identyfikatorami CVE, błędów konfiguracji, przypadków ujawnienia informacji oraz innych zagrożeń występujących w usługach i systemach informatycznych.
2. Wykorzystywać mechanizm skanowania oparty na deklaratywnych szablonach detekcyjnych zapisanych w formacie YAML, umożliwiających definiowanie żądań, warunków wykrywania zagrożeń, metod weryfikacji oraz metadanych identyfikowanych podatności.
3. Umożliwiać samodzielne tworzenie, edytowanie, walidację oraz uruchamianie własnych szablonów testowych bez konieczności modyfikowania kodu źródłowego silnika skanującego.
4. Zapewniać dostęp do aktualizowanej bazy szablonów detekcyjnych, zawierającej testy identyfikujące znane podatności, błędy konfiguracji, nieprawidłowo zabezpieczone usługi oraz zagrożenia dotyczące aplikacji i urządzeń sieciowych.
5. Umożliwiać niezależną aktualizację silnika skanującego oraz bazy szablonów detekcyjnych.
6. Obsługiwać wykonywanie testów dla co najmniej następujących protokołów i usług: HTTP, HTTPS, DNS, TCP oraz SSL/TLS.
7. Umożliwiać skanowanie pojedynczych adresów IP, domen, adresów URL, zakresów adresacji IP oraz list zasobów wskazanych przez Zamawiającego.
8. Umożliwiać wykonywanie testów bezpieczeństwa aplikacji internetowych i interfejsów API, w tym obsługę specyfikacji OpenAPI/Swagger.

9. Umożliwiać klasyfikację i filtrowanie wyników według poziomów istotności: Informational, Low, Medium, High oraz Critical.
10. Umożliwiać selektywne uruchamianie szablonów i kategorii testów na podstawie identyfikatorów, tagów, poziomów istotności oraz typów protokołów.
11. Zapewniać możliwość definiowania wieloetapowych scenariuszy testowych (workflow), w których wykonanie kolejnych testów może zależeć od wyników wcześniejszych etapów.
12. Umożliwiać uruchamianie skanowania z poziomu interfejsu wiersza poleceń (CLI) oraz automatyzowanie procesu skanowania za pomocą skryptów i harmonogramów systemowych.
13. Umożliwiać integrację z zewnętrznymi narzędziami automatyzacji, systemami raportowania oraz rozwiązaniami bezpieczeństwa za pośrednictwem interfejsu CLI i ustrukturyzowanych formatów danych.
14. Obsługiwać eksport wyników skanowania co najmniej do formatów JSON, JSONL oraz SARIF.
15. Umożliwiać ograniczanie liczby żądań wysyłanych w jednostce czasu, konfigurację współbieżności testów oraz określanie limitów czasu wykonywania żądań.
16. Umożliwiać wykluczanie określonych adresów, zasobów, szablonów i kategorii testów z procesu skanowania.
17. Umożliwiać instalację i uruchomienie silnika skanującego lokalnie, w infrastrukturze Zamawiającego, bez konieczności korzystania z zewnętrznej platformy chmurowej w celu realizacji podstawowych funkcji skanowania.
18. Zapewniać możliwość wykonywania skanowania bez obowiązkowego przekazywania wyników oraz informacji o skanowanych zasobach do zewnętrznych usług. Ewentualne funkcje wymagające komunikacji z usługami zewnętrznymi muszą być możliwe do wyłączenia.
19. Umożliwiać wykonywanie skanowań cyklicznych przy wykorzystaniu zewnętrznego harmonogramu, np. harmonogramu systemu operacyjnego.
20. Umożliwiać uruchamianie skanowania z wykorzystaniem własnych konfiguracji przeznaczonych dla różnych grup zasobów i poziomów intensywności testowania.

Wymagania dotyczące bezpieczeństwa środowiska OT/SCADA

Ze względu na specyfikę infrastruktury wodociągowo-kanalizacyjnej rozwiązanie musi umożliwiać kontrolowanie zakresu i intensywności skanowania w sposób ograniczający ryzyko zakłócenia działania systemów produkcyjnych oraz technologicznych.
W szczególności wymagane jest:

1. Możliwość wykluczenia ze skanowania wskazanych systemów sterowania przemysłowego, sterowników PLC, urządzeń automatyki przemysłowej, stacji operatorskich i systemów SCADA.
2. Możliwość ograniczenia intensywności skanowania poprzez określenie maksymalnej liczby żądań na sekundę oraz poziomu współbieżności testów.

3. Możliwość definiowania odrębnych profili skanowania dla infrastruktury biurowej IT, serwerowej oraz systemów wspierających procesy technologiczne.
4. Możliwość wykluczania testów mogących powodować zakłócenia w dostępności usług lub zmiany konfiguracji testowanych systemów.
5. Możliwość uruchamiania wyłącznie wybranych, uprzednio zatwierdzonych szablonów detekcyjnych.
6. Możliwość wykonywania skanowania w określonych przez Zamawiającego oknach serwisowych.

Aktywne skanowanie urządzeń OT, sterowników PLC i systemów SCADA może być realizowane wyłącznie po przeprowadzeniu oceny ryzyka, uzgodnieniu zakresu i metody testów z Zamawiającym oraz uzyskaniu jego odrębnej zgody. W przypadku braku takiej zgody zasoby te muszą zostać wyłączone z aktywnego skanowania.

Wymagania wdrożeniowe

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

1. Instalacji i konfiguracji narzędzia w środowisku wskazanym przez Zamawiającego.
2. Instalacji aktualnej, stabilnej wersji silnika skanującego.
3. Konfiguracji mechanizmu aktualizacji bazy szablonów detekcyjnych.
4. Przygotowania co najmniej trzech profili skanowania:
    - podstawowego, przeznaczonego do cyklicznej identyfikacji typowych podatności i błędów konfiguracji;
    - rozszerzonego, obejmującego szerszy zakres testów bezpieczeństwa infrastruktury IT;
    - krytycznego, ukierunkowanego na identyfikację podatności o poziomie High i Critical.
5. Przygotowania konfiguracji umożliwiającej ograniczenie intensywności skanowania i wykluczenie wskazanych zasobów technologicznych.
6. Konfiguracji eksportu wyników do formatów umożliwiających dalsze przetwarzanie i raportowanie.
7. Przeprowadzenia testowego skanowania zasobów wskazanych przez Zamawiającego.
8. Przekazania dokumentacji technicznej, instalacyjnej i eksploatacyjnej.
9. Przeprowadzenia instruktażu dla administratorów Zamawiającego obejmującego uruchamianie skanowania, aktualizację szablonów, interpretację wyników oraz tworzenie własnych reguł detekcyjnych.

Wymagania licencyjne

Rozwiązanie musi umożliwiać lokalne wykorzystanie silnika skanującego bez obowiązku wykupienia subskrypcji usługi chmurowej.

Zamawiający dopuszcza wykorzystanie oprogramowania open source, o ile jego licencja zezwala na planowany sposób wykorzystywania rozwiązania.

Wykonawca musi zapewnić legalność wykorzystania oprogramowania oraz przekazać informacje dotyczące obowiązujących warunków licencyjnych.

Zamawiający dopuszcza zaoferowanie dowolnego rozwiązania spełniającego wszystkie minimalne wymagania funkcjonalne i techniczne określone w niniejszym opisie przedmiotu zamówienia.
Wykonawca zobowiązany jest do wykazania spełnienia wymagań poprzez przedstawienie dokumentacji technicznej rozwiązania oraz, na żądanie Zamawiającego, demonstrację wymaganych funkcjonalności.

Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązań z zakresu bezpieczeństwa w tym usług HA (Serwer pod skaner podatności)

Serwer fizyczny - 1 sztuka

Szczegółowy opis		
Serwer W ofercie (przedmiotowe środki dowodowe) należy podać nazwę producenta, typ, model oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Nie dopuszcza się zaoferowania komputera odnawianego.		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**
1.	Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
2.	Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – minimum16. Minimalna częstotliwość pracy procesora 2.3 GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora nie powinien być niższy niż 370 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta.
3.	Liczba zainstalowanych procesorów	2
4.	Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
5.	Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. Zainstalowane kości o pojemności min. 32GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
6.	Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
7.	Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
8.	Rozbudowa dysków	Zainstalowane 6 dysków SSD PCIe 4.0 x4 o pojemności minimum 1960GB każdy. Dyski muszą mieć możliwość wymiany na gorąco. Wymagany jest wewnętrzny slot na kartę Micro SD.

9.	Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS 12Gb. Kontroler musi posiadać 4GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID - 0/1/10/5/50/6/60.
10.	Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1200W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
11.	Interfejsy sieciowe	Zainstalowane dwuportowa karta 10/25GbE z obsługą złącza SFP. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
12.	Sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 x8 z czego jeden High-Profile, 1 slot OCP Gen5 oraz jeden slot PCIe wewnątrz obudowy serwera dedykowany pod kontroler dyskowy.
13.	Dodatkowe porty	• z przodu obudowy: 2x USB 3 (z czego jeden z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny, port Mini DisplayPort • z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
14.	Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1. Serwer w obecnej konfiguracji musi być przystosowany, aby mógł pracować w temperaturze otoczenia 25 stopni Celsjusza, wykorzystując pełne możliwości (bez Throttlingu).
15.	Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI

		• Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie

		oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
16.	Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.
17.	Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.

18.	Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
19.	Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu powinno odbywać się poprzez dedykowany port USB na froncie serwera. Wymaga się aby serwer posiadał diody sygnalizacyjne awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
20.	Systemy operacyjne	System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich; System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. Zabrania się instalowania lub preinstalowania systemu operacyjnego w jakimkolwiek środowisku wirtualnym. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta. MS Windows Server 2025 Standard wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym wcześniej kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji firmy Microsoft® wraz z licencjami dostępowymi CAL dla 40 użytkowników lub równoważny. Warunki równoważności: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny Active Directory na poziomie Microsoft Windows Server 2019 5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

		a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10. 11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre . 12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP 13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra. 16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra. 17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6; 20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1 ; 23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory. 24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). Wymagania dla równoważnych licencji dostępowych dla urządzenia: - Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu Device Cal z wdrożoną rolą Active Directory. - Każda z licencji musi pozwalać na dostęp wielu użytkowników z jednego, licencjonowanego urządzenia do zasobów serwera. W przypadku zaproponowania przez Dostawcę oprogramowania równoważnego zobowiązuje się on do: – wdrożenia oprogramowania oraz przeprowadzenia certyfikowanych szkoleń dla użytkowników oferowanego rozwiązania w wymiarze co najmniej 40 godzin. – 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.
21.	Gwarancja	• Całe rozwiązanie musi być objęte minimum 24 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem reakcji do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy, • Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej i pozostają własnością Zamawiającego, • Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, • Serwer musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się dostarczenia serwera odnawianego, demonstracyjnych lub powystawowych, • Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia, • Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje, • Zamawiający wymaga stosownego oświadczenia producenta macierzy lub jego oddziału w Polsce potwierdzającego spełnienie powyższych warunków.
22.	Certyfikaty, oświadczenia i standardy	• Deklaracja zgodności CE, • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki, • Certyfikat ISO 9001 dla producenta komputera lub równoważny, • Certyfikat ISO 14001 dla producenta komputera lub równoważny, • Certyfikat ISO 50001 dla producenta komputera lub równoważny, Wymagane certyfikaty należy dołączyć do oferty. Zamawiający dopuszcza dołączenie dokumentów w języku angielskim.

Macierz dyskowa. Zakup i skonfigurowanie macierzy RAID w serwerach kopii zapasowych.

W ramach dostawy Wykonawca zapewni oprogramowanie do wykonywania kopii zapasowych wraz z licencją na okres nie krótszy niż 24 miesięcy, kompatybilne z systemami eksploatowanymi przez Zamawiającego oraz dopuszczone do stosowania przez producenta systemu sterowania. Serwer zostanie umieszczony w dedykowanym segmencie sieciowym i będzie administrowany z wykorzystaniem kont niezależnych od domeny sieci biurowej, tak aby

kompromitacja sieci biurowej nie skutkowała uzyskaniem dostępu do kopii zapasowych. Okres gwarancji na serwer wyniesie nie mniej niż 24 miesiące.

Przedmiotem zamówienia jest dostawa fabrycznie nowego, sieciowego serwera pamięci masowej NAS, wraz z 4 dyskami twardymi o pojemności min 8 TB każdy, przeznaczonymi do pracy ciągłej w środowisku serwerowym.
Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja 1 sztuki serwera plików NAS, wyposażonego w minimum 4 zatoki z dyskami twardymi min 8TB każdy. Konfiguracja zgodna z wytycznymi zamawiającego.
Urządzenie będzie wykorzystywane do bezpiecznego przechowywania danych oraz wykonywania i przechowywania kopii zapasowych systemów informatycznych Zamawiającego.

Serwer NAS wraz z 4 dyskami - Minimalne wymagania techniczne

Oferowane urządzenie musi spełniać następujące wymagania:

- Obudowa rack 19", wysokość minimum 1U,
- Procesor AMD Ryzen V1500B, 4 rdzenie, 8 wątków, taktowanie 2,2 GHz lub parametry równoważne,
- Pamięć RAM: minimum 4 GB DDR4 ECC SODIMM, z możliwością rozbudowy do minimum 32 GB,
- Minimum 4 wewnętrzne zatoki na dyski 3,5" SATA HDD lub 2,5" SATA SSD,
- Obsługa wymiany dysków podczas pracy urządzenia (hot-swap),
- Minimum 4 porty sieciowe RJ-45 1GbE,
- Minimum 2 porty USB 3.2 Gen 1,
- Minimum 1 port rozszerzeń umożliwiający podłączenie kompatybilnej jednostki rozbudowy,
- Minimum 1 gniazdo PCIe do instalacji kompatybilnych kart rozszerzeń,
- Obsługa macierzy RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, JBOD,
- System operacyjny umożliwiający zarządzanie przestrzenią dyskową, użytkownikami, uprawnieniami, folderami współdzielonymi oraz kopiami zapasowymi,
- Obsługa protokołów sieciowych SMB, NFS, FTP oraz iSCSI,
- Możliwość rozbudowy przestrzeni dyskowej przy użyciu kompatybilnej jednostki rozszerzającej,
- Urządzenie wyposażone w szyny rack do montażu w szafie RACK 19”,
- Urządzenie musi być wyposażone w zasilacze redundantne,
- Urządzenie przeznaczone do pracy ciągłej 24/7,
- Model dysku musi być w pełni kompatybilny i zgodny z serwerem NAS,
- Pojemność - minimum 8 TB,
- Typ: dysk twardy HDD klasy enterprise, przeznaczony do pracy ciągłej w serwerach NAS oraz pracy w macierzach RAID,
- Format: 3,5 cala.
- Interfejs: SATA.
- Dyski fabrycznie nowe, nieużywane, objęte gwarancją producenta.

Wymagania dotyczące dostawy i zakres wdrożenia

Wykonawca zobowiązany jest do:

- Dostawy fabrycznie nowego jednego serwera NAS oraz czterech dysków twardych o pojemności min 8TB każdy,
- Instalacja wszystkich dysków w zatokach serwera,
- Uruchomienie urządzenia i konfiguracja podstawowych parametrów systemowych,
- Skonfigurowanie macierzy RAID zgodnie z wymaganiami zamawiającego,
- Dostarczenie dokumentacji oraz informacji dotyczących gwarancji,
- Dostarczenie urządzenia kompletnego i gotowego do wdrożenia.

Gwarancja

- Wymagana gwarancja na serwer NAS: minimum 24 miesiące,
- W okresie gwarancji Wykonawca zapewni możliwość zgłaszania usterek oraz realizację napraw lub wymian zgodnie z warunkami gwarancji,
- Wszystkie elementy zestawu muszą być fabrycznie nowe, nieużywane i kompatybilne ze sobą,

Warunkiem odbioru będzie:

1. Dostarczenie i uruchomienie kompletnego urządzenia NAS.
2. Potwierdzenie obecności dysków HDD odebranych od Zamawiającego.
3. Potwierdzenie prawidłowej konfiguracji macierzy RAID.
4. Weryfikacja dostępu do udostępnionych zasobów sieciowych.
5. Potwierdzenie działania monitorowania stanu dysków.
6. Przekazanie dokumentacji i informacji gwarancyjnych.

Wykonanie przeglądu konfiguracji PC, serwerów i urządzeń sieciowych

Celem zadania jest sprawdzenie czy urządzenia sieci technologicznej są ustawione bezpiecznie i jednolicie, oraz poprawienie w sposób, który nie zakłóci pracy instalacji.

Wykonawca najpierw sporządzi lub zaktualizuje inwentaryzację urządzeń OT. Obejmie ona stacje operatorskie (HMI), stacje inżynierskie, serwery SCADA i historian, sterowniki (PLC, RTU), zabezpieczenia i urządzenia pomiarowe, przełączniki, routery i firewalle przemysłowe. Dla każdego urządzenia zostaną ustalone: producent, model, wersja oprogramowania lub firmware'u, funkcja w procesie oraz osoba odpowiedzialna.

Następnie Wykonawca uzgodni z Zamawiającym wzorzec bezpiecznych ustawień dla każdego rodzaju urządzeń. Wzorzec będzie oparty na wytycznych producentów systemów sterowania, normie IEC 62443 (w szczególności 3-3 i 4-2) oraz uznanych dobrych praktykach, np. CIS. Wzorzec uwzględni wymagania producenta aplikacji przemysłowych, tak aby zmiany nie naruszały gwarancji ani certyfikacji systemu.

Zakup 4 szt. – zarządzalnych przełączników sieciowych Multigigabit PoE++

Przedmiotem zamówienia jest dostawa zarządzalnego przełącznika sieciowego warstwy L2/L3, przeznaczonego do budowy i rozbudowy infrastruktury sieciowej LAN, z obsługą wielogigabitowej transmisji danych oraz zasilania urządzeń końcowych za pośrednictwem Ethernet (PoE).

Minimalne wymagania techniczne:

- 24 porty miedziane Ethernet RJ-45 obsługujące przepustowość 2,5 Gb/s.
- 16 portów z obsługą PoE+ o mocy do 30 W na port.
- 8 portów z obsługą PoE++ o mocy do 60 W na port.
- Łączny budżet mocy PoE nie mniejszy niż 700 W.
- 4 porty uplink typu SFP28, obsługujące transmisję 10 Gb/s; obsługa 25 Gb/s w trybie stackingu, zgodnie ze specyfikacją urządzenia.
- Funkcje zarządzania ruchem sieciowym, w tym obsługa sieci VLAN, agregacji łączy, protokołów STP/RSTP/MSTP oraz mechanizmów QoS.
- Obsługa mechanizmów bezpieczeństwa sieciowego, w tym kontroli dostępu do portów i uwierzytelniania 802.1X.
- Możliwość zarządzania przez interfejs WWW oraz CLI.
- Obsługa protokołów zarządzania i monitorowania sieci, w tym SNMP i SSH.
- Możliwość montażu w standardowej szafie rack 19".
- Zasilanie z sieci elektrycznej 230 V AC.
- Urządzenie fabrycznie nowe, kompletne, gotowe do instalacji i konfiguracji.

Zamawiający dopuszcza rozwiązania równoważne, pod warunkiem spełnienia wszystkich określonych wymagań technicznych lub parametrów lepszych oraz zapewnienia współpracy z posiadaną infrastrukturą sieciową.

Zakup 10 szt. - wkładki optyczne SFP28 LR 10/25GbE

Przedmiotem zamówienia jest dostawa wkładek optycznych typu SFP28 LR, przeznaczonych do transmisji danych w sieciach Ethernet z szybkością 10 Gb/s oraz 25 Gb/s.

Minimalne wymagania techniczne:

- Typ modułu: SFP28 LR,
- Obsługiwane szybkości transmisji: 10 Gb/s i 25 Gb/s (Dual Rate),
- Długość fali optycznej: 1310 nm,
- Zasięg transmisji: do 10 km,
- Złącze optyczne: LC Duplex,
- Typ włókna światłowodowego: jednomodowe (SMF),
- Przeznaczenie: transmisja danych w sieciach Ethernet 10GbE i 25GbE,
- Zgodność z odpowiednimi standardami transmisji Ethernet dla obsługiwanych szybkości,
- Kompatybilność z urządzeniami sieciowymi wyposażonymi w odpowiednie porty SFP28, zgodnie z wymaganiami technicznymi tych urządzeń,
- Moduł fabrycznie nowy, kompletny i wolny od wad.

Zamawiający dopuszcza rozwiązania równoważne, pod warunkiem spełnienia wszystkich określonych wymagań technicznych oraz zapewnienia prawidłowej współpracy z posiadaną infrastrukturą sieciową.

Przegląd będzie prowadzony metodami nieinwazyjnymi. Aktywne skanowanie sterowników i urządzeń sieci procesowej będzie dopuszczalne tylko za zgodą Zamawiającego, w oknie serwisowym albo na środowisku testowym. W pozostałych przypadkach Wykonawca oprze się na odczycie konfiguracji, dokumentacji i pasywnej analizie ruchu.

Przegląd obejmie między innymi:

- stacje i serwery: konta z uprawnieniami administratora, konta współdzielone i automatyczne logowanie, zbędne usługi i otwarte porty, udziały sieciowe, ochronę przed złośliwym oprogramowaniem (w tym kontrolę uruchamianych aplikacji tam, gdzie klasyczny antywirus nie jest wspierany przez producenta), kontrolę nośników USB, stan aktualizacji, szyfrowanie dysków tam, gdzie jest możliwe, oraz rejestrowanie zdarzeń;
- sterowniki i urządzenia polowe: hasła domyślne, ochronę programu i konfiguracji hasłem, położenie przełącznika trybu pracy (RUN/PROGRAM), wersje firmware'u względem znanych podatności, zbędne usługi (np. serwery WWW, FTP, Telnet, SNMP v1/v2c) oraz dozwolone źródła komunikacji;
- urządzenia sieciowe: hasła domyślne, protokoły zarządzania, nieużywane porty, separację sieci VLAN, synchronizację czasu i rejestrowanie zdarzeń;
- kopie zapasowe: istnienie i aktualność kopii programów sterowników, konfiguracji urządzeń i obrazów stacji oraz możliwość ich odtworzenia.

Zamawiający otrzyma raport z listą stwierdzonych odstępstw wraz z oceną ich wagi. Ocena uwzględni znaczenie urządzenia dla procesu i bezpieczeństwa instalacji.
Wykonawca usunie odstępstwa uzgodnione z Zamawiającym. Zmiany będą wprowadzane w uzgodnionych oknach serwisowych, po wykonaniu kopii zapasowej, z planem wycofania i tam gdzie to wymagane, po akceptacji producenta systemu. Każda zmiana zostanie udokumentowana. Odstępstw, których nie da się usunąć ze względu na wymagania aplikacji, przestarzały system operacyjny lub brak wsparcia producenta, Wykonawca nie pozostawi bez opisu. Opisze je wraz z propozycją zabezpieczeń kompensujących, np. dodatkowej izolacji sieciowej, kontroli uruchamianych aplikacji czy monitorowania, do formalnej akceptacji ryzyka przez Zamawiającego.

Przeprowadzenie aktualizacji oprogramowania
W ramach zadania wszystkie systemy mają zostać doprowadzone do wersji wspieranych przez producentów.
Wykonawca zaktualizuje systemy operacyjne stanowisk i serwerów, oprogramowanie układowe przełączników, firewalli, punktów dostępowych i macierzy oraz standardowe aplikacje biurowe. Aktualizacje serwerów i urządzeń sieciowych będą poprzedzone wykonaniem kopii zapasowej i sprawdzeniem, czy nowa wersja jest zgodna z aplikacjami Zamawiającego.
Dla urządzeń i systemów, które utraciły wsparcie producenta lub nie mogą zostać zaktualizowane, Wykonawca sporządzi listę zawierającą dla każdej pozycji: opis urządzenia,

jego funkcję w procesie, przyczynę braku możliwości aktualizacji, znane podatności oraz ocenę ryzyka. Dla każdej pozycji Wykonawca przedstawi rekomendację: wymianę z orientacyjnym terminem i zakresem prac albo pozostawienie w eksploatacji z zabezpieczeniami kompensującymi.

W sieci OT poprawki nie będą instalowane automatycznie bez kontroli, ponieważ niezweryfikowana aktualizacja może zakłócić pracę instalacji. Wykonawca uruchomi mechanizm kontrolowanego zarządzania poprawkami, obejmujący:

- serwer dystrybucji poprawek umieszczony w strefie pośredniczącej (IDMZ), pobierający poprawki z zewnątrz i udostępniający je do sieci OT, bez bezpośredniego dostępu urządzeń OT do Internetu;
- automatyczne pobieranie poprawek i raportowanie stanu aktualności wszystkich stacji i serwerów OT;
- instalację poprawek wyłącznie zatwierdzonych przez producenta systemu sterowania jako zgodne z eksploatowaną wersją, po testach na środowisku testowym lub stacji zapasowej, w uzgodnionych oknach serwisowych, z możliwością wycofania;
- automatyczną instalację poprawek tam, gdzie Zamawiający uzna to za bezpieczne, np. na stacjach poza bezpośrednim sterowaniem procesem;
- regularne śledzenie komunikatów bezpieczeństwa producentów oraz CERT, z oceną, czy dotyczą urządzeń Zamawiającego, także sterowników, urządzeń sieciowych i firmware'u, dla których aktualizacja odbywa się ręcznie;
- aktualizację sygnatur ochrony przed złośliwym oprogramowaniem przez ten sam serwer pośredniczący.

Wykonawca opisze procedurę obsługi mechanizmu, określającą role i odpowiedzialność, częstotliwość przeglądu nowych poprawek (co najmniej raz w miesiącu), sposób uzyskania zgody producenta systemu, testowania, zatwierdzania i wycofywania poprawek, tryb postępowania w przypadku krytycznych podatności, sposób dokumentowania wprowadzonych zmian oraz okresową aktualizację listy urządzeń bez wsparcia. Procedura i mechanizm zostaną przekazane Zamawiającemu wraz z przeszkoleniem wskazanych pracowników, tak aby stan aktualności utrzymywał się po zakończeniu zamówienia.

Wykonanie kopii zapasowych i uruchomienie regularnego procesu

Wykonawca zinwentaryzuje z Zamawiającym, które systemy i dane podlegają ochronie – co najmniej serwery, bazy danych, systemy dziedzinowe, zasoby plikowe, poczta i konfiguracje urządzeń sieciowych – oraz reguły kopii zapasowych (utrata danych, przestój).

Dla urządzeń i systemów, które utraciły wsparcie producenta lub nie mogą zostać zaktualizowane, Wykonawca sporządzi wykaz zawierający ocenę ryzyka oraz rekomendację wymiany albo dalszej eksploatacji z zastosowaniem zabezpieczeń kompensujących.

Uzupełnienie inwentaryzacji aktywów IT

Zamawiający otrzyma pełny i aktualny wykaz swojego sprzętu i oprogramowania.

Wykonawca zweryfikuje istniejącą ewidencję przez przeskanowanie sieci i oględziny na miejscu, w biurze i na SUW. Dla każdego urządzenia rejestr będzie zawierał co najmniej nazwę, rodzaj, producenta i model, numer seryjny, lokalizację, adres sieciowy, wersję systemu, osobę odpowiedzialną oraz informację, czy producent nadal je wspiera. Rejestr obejmie również zainstalowane oprogramowanie i posiadane licencje.
Urządzenia, których pochodzenia lub przeznaczenia nie uda się ustalić, Wykonawca wskaże Zamawiającemu osobno. Rejestr zostanie przekazany w edytowalnym pliku wraz z aktualnymi schematami sieci i prostą procedurą jego bieżącego uzupełniania.

Przegląd sposobu zarządzania hasłami i dostępami

Zadanie ma doprowadzić do stanu, w którym każda osoba ma dostęp tylko do tego, czego potrzebuje, a hasła są silne i nie są współdzielone.
Wykonawca przejrzy wszystkie konta użytkowników, administratorów i konta techniczne na serwerach, urządzeniach sieciowych i w najważniejszych aplikacjach. Wskaże konta nieużywane, współdzielone, z hasłami domyślnymi lub nigdy niezmienianymi oraz z uprawnieniami szerszymi niż potrzebne, a po uzgodnieniu z Zamawiającym usunie je lub ograniczy.
Następnie wdroży jednolitą politykę haseł: minimalną długość, blokadę konta po kilku nieudanych próbach i zakaz powtarzania poprzednich haseł. Administratorzy otrzymają osobne konta do zadań administracyjnych, inne niż do codziennej pracy, oraz menedżer haseł do bezpiecznego przechowywania haseł serwisowych. Zamawiający otrzyma procedury nadawania i odbierania uprawnień oraz ich okresowego przeglądu.

Wdrożenie MFA dla dostępów administracyjnych

Uwierzytelnianie wieloskładnikowe obejmie zdalny dostęp VPN oraz logowanie administratorów do serwerów, firewalli i urządzeń sieciowych, konsoli systemu kopii zapasowych i poczty. Drugim składnikiem będzie aplikacja na telefonie lub sprzętowy klucz bezpieczeństwa; kody SMS nie będą jedyną dopuszczoną metodą. Urządzenia, które nie obsługują MFA, będą administrowane za pośrednictwem stanowiska pośredniczącego objętego tym zabezpieczeniem.

Zadanie 4 - Obszar techniczny OT

WDROŻENIE PRZEMYSŁOWEGO SYSTEMU IDS

Przedmiotem zamówienia jest:

1. Wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. Dostawa licencji oraz sond sprzętowych,
3. Udzielenie wsparcia dla administratorów Zamawiającego,
4. Organizacja i realizacja szkoleń dla administratorów Zamawiającego.

Funkcjonalność i specyfikacja

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:

a) pasywne monitorowanie sieci przemysłowej Zamawiającego,
b) automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
c) szczegółową inwentaryzację urządzeń,
d) automatyczne odzwierciedlenie połączeń komunikacyjnych,
e) informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
f) wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
g) budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
h) obsługę LLDP, CDP, CIP, SSDP.

10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.

15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)
20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:

a) malware/”zero-day”,
b) atak DOS/DDOS,
c) atak typu ATP,
d) spyware, skanowanie sieci,
e) zagrożenia Man-in-the-Middle,
f) anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
g) wykrywanie połączeń do innej sieci LAN/internet,
h) wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.

29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.

35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40. Wykonawca dostarczy:
    licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
    gwarancję producenta.
41. Serwis producenta systemu IDS ma obejmować:

a) Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
b) Dostęp do nowych wersji systemu IDS.
c) Dostęp do aktualizacji i poprawek systemu IDS.
d) Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
e) Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
f) Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

42. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
43. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
44. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
45. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
46. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
47. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
48. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w dniu zawarcia umowy pomiędzy Zamawiającym a Wykonawcą.

49. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

Sprzętowe sondy do monitorowania sieci OT

Przedmiotem zamówienia jest dostawa kompletu sond sprzętowych obsługujących infrastrukturę OT Zamawiającego. Zamawiający posiada obecnie następującą infrastrukturę:

1. Monitoring i sterowanie stacji uzdatniania wody (TelWin)
2. Monitoring i sterowanie przepompowniami zlokalizowanymi w Konstantynowie Łódzkim (akt. 16+ lokalizacji) komunikujących się z systemem SCADA dzięki kartom SIM (producent Control System).
3. Dwa różne systemy SCADA do obsługi w/w infrastruktury pracujące na dwóch stacjach roboczych (Windows 11 Pro i Windows 7 – w trakcie wymiany na Windows 11 Pro).

Wymagania:

1. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
2. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
3. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
4. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
5. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
6. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
7. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
8. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
9. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
10. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
11. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
12. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
13. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.
14. Wykonawca dostarczy:
    - sondy sprzętowe w liczbie *(do decyzji Wykonawcy po wizji lokalnej)* ... szt. do monitorowania sieci przemysłowej,
    - gwarancję producenta.

15. Serwis producenta ma obejmować:
    - Dostęp do aktualizacji oprogramowania sond sprzętowych.
    - Wymianę uszkodzonych sond sprzętowych w razie awarii.
    - Przekazanie danych kontaktowych do działu technicznego producenta.
    - Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
16. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
17. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
18. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

Dostawa i wdrożenie systemu monitorowania sieci przemysłowej (OT)

Przedmiotem zamówienia jest:

1. Wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. Dostawa licencji oraz sond sprzętowych,
3. Udzielenie wsparcia dla administratorów Zamawiającego,
4. Organizacja i realizacja szkoleń dla administratorów Zamawiającego.

WDROŻENIE I ZAKUP URZĄDZENIA ZABEZPIECZAJĄCEGO SIEĆ TYPU NGFW DLA OT/IT

Na styku sieci biurowej i sieci sterowania SUW zostanie zainstalowany dedykowany firewall, niezależny od firewalla chroniącego połączenie z Internetem.

Wykonawca dostarczy i skonfiguruje urządzenie, które rozpoznaje protokoły przemysłowe używane na SUW i pozwala ograniczyć komunikację do konkretnych urządzeń i operacji. Oprogramowanie będzie objęte aktualizacjami i wsparciem producenta przez co najmniej 12 miesięcy. Musi zawierać:

- roczną usługę wsparcia serwisowego dla urządzenia (wsparcie w dni robocze, przez 8 godzin dziennie, 5 dni w tygodniu, Next Business Day – docelowa dostawa sprzętu zamiennego następnego dnia roboczego, zgodnie z warunkami usługi),
- roczną subskrypcje licencyjną zapewniająca zaawansowaną ochronę przed złośliwym oprogramowaniem dla zapory sieciowej z oprogramowaniem Threat Defense, (wykrywanie i blokowanie złośliwego oprogramowania w plikach przesyłanych przez sieć, sprawdzanie plików pod kątem zagrożeń, dostęp do usług analizy bezpieczeństwa w okresie aktywnej subskrypcji),

- roczną subskrypcję funkcji bezpieczeństwa dla urządzenia pracującego z oprogramowaniem Threat Defense (FTD), (wykrywanie i blokowanie prób włamań oraz znanych ataków sieciowych, filtrowanie ruchu na podstawie informacji o znanych zagrożeniach, dostęp do aktualizacji związanych z subskrypcją przez okres jej obowiązywania).

Firewall będzie domyślnie blokował cały ruch i przepuszczał wyłącznie połączenia uzgodnione z Zamawiającym. Będzie zarządzany z osobnych kont, innych niż konta administratorów sieci biurowej, a zdarzenia będą rejestrowane przez co najmniej 90 dni. Urządzenie umożliwi w przyszłości podłączenie systemu monitorującego ruch w sieci sterowania.
Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia zabezpieczającego sieć typu Next-Generation Firewall (NGFW), wraz z oprogramowaniem, wymaganymi licencjami, subskrypcjami oraz wyposażeniem niezbędnym do prawidłowego uruchomienia i eksploatacji.

Minimalne wymagania techniczne i funkcjonalne:

1. Urządzenie musi zapewniać funkcjonalność zapory sieciowej nowej generacji (NGFW).
2. Urządzenie musi obsługiwać kontrolę ruchu sieciowego z uwzględnieniem adresów IP, portów, protokołów, aplikacji oraz zdefiniowanych polityk bezpieczeństwa.
3. Urządzenie musi zapewniać kontrolę stanową połączeń (Stateful Firewall).
4. Urządzenie musi umożliwiać identyfikację aplikacji sieciowych oraz kontrolę ruchu na poziomie aplikacji (Application Visibility and Control).
5. Urządzenie musi posiadać system wykrywania i zapobiegania włamaniom (IPS), z możliwością aktualizacji sygnatur zagrożeń.
6. Przepustowość urządzenia przy aktywnych funkcjach zapory sieciowej, kontroli aplikacji oraz IPS musi wynosić co najmniej 1,5 Gb/s.
7. Urządzenie musi obsługiwać szyfrowane połączenia VPN IPsec, z przepustowością co najmniej 1,2 Gb/s.
8. Urządzenie musi umożliwiać inspekcję szyfrowanego ruchu TLS.
9. Przepustowość inspekcji ruchu TLS musi wynosić co najmniej 0,7 Gb/s, zgodnie zsRNtx7zK metodologią pomiarową producenta.
10. Urządzenie musi obsługiwać co najmniej 30 000 równoczesnych sesji oraz 6 000 nowych połączeń na sekundę przy aktywnej kontroli aplikacji.
11. Urządzenie musi umożliwiać zestawienie co najmniej 50 równoczesnych połączeń VPN, z uwzględnieniem oferowanych licencji.
12. Urządzenie musi obsługiwać konfigurację wysokiej dostępności w trybie Active/Standby.
13. Urządzenie musi posiadać co najmniej:
    - 4 porty Ethernet 1 Gb/s RJ-45,
    - 1 port SFP 1 Gb/s,
    - 1 dedykowany port zarządzający Ethernet 1 Gb/s,
    - port konsolowy RJ-45,
    - port USB Type-C,
    - port USB Type-A.

14. Urządzenie musi posiadać pamięć masową o pojemności co najmniej 64 GB.
15. Urządzenie musi umożliwiać zarządzanie i konfigurację za pomocą interfejsu administracyjnego oraz monitorowanie zdarzeń bezpieczeństwa i ruchu sieciowego.
16. Urządzenie musi umożliwiać rejestrowanie zdarzeń, tworzenie raportów oraz definiowanie i egzekwowanie polityk bezpieczeństwa.
17. Urządzenie musi posiadać pasywny system chłodzenia, bez wentylatorów.
18. Urządzenie musi być zasilane napięciem 100–240 V AC, 50–60 Hz, za pośrednictwem zewnętrznego zasilacza.
19. Wykonawca musi dostarczyć wszystkie niezbędne licencje i subskrypcje umożliwiające korzystanie z wymaganych funkcji bezpieczeństwa.
20. W ramach zamówienia należy zapewnić dostęp do aktualizacji oprogramowania oraz sygnatur bezpieczeństwa przez okres wskazany przez Zamawiającego.
21. Urządzenie musi być fabrycznie nowe, nieużywane i objęte gwarancją producenta przez okres określony w dokumentacji zamówienia.
22. Dostawa musi obejmować komplet wyposażenia niezbędnego do uruchomienia urządzenia oraz dokumentację techniczną.

Wymagania dotyczące zgodności:

Zamawiający dopuszcza rozwiązania równoważne, pod warunkiem spełnienia wszystkich minimalnych wymagań technicznych i funkcjonalnych określonych w opisie przedmiotu zamówienia. Wykonawca zobowiązany jest wykazać zgodność oferowanego rozwiązania z wymaganiami na podstawie dokumentacji technicznej producenta.

Warunki dostawy:

Przedmiot zamówienia zostanie dostarczony jako kompletny zestaw gotowy do instalacji i konfiguracji, wraz z wymaganymi licencjami, subskrypcjami, akcesoriami oraz dokumentacją techniczną.

Poufność, bezpieczeństwo informacji i dane osobowe

- Wszystkie informacje o infrastrukturze Zamawiającego, topologii sieci, adresacji, podatnościach, zdarzeniach bezpieczeństwa, konfiguracji, procedurach i wynikach analizy stanowią informacje poufne.
- Wykonawca nie może ujawniać, publikować ani wykorzystywać danych i wyników analizy do celów marketingowych, sprzedażowych, badawczych lub referencyjnych bez uprzedniej zgody Zamawiającego. Ewentualne wykorzystanie danych może nastąpić wyłącznie w postaci zanonimizowanej i w zakresie zaakceptowanym przez Zamawiającego.
- Wykonawca powinien zabezpieczać dane uzyskane w toku realizacji zamówienia przed dostępem osób nieuprawnionych, w szczególności poprzez kontrolę dostępu, szyfrowanie nośników lub plików oraz ograniczenie dostępu wyłącznie do osób realizujących usługę.
- Jeżeli w toku realizacji usługi dojdzie do przetwarzania danych osobowych, Strony określą właściwą podstawę i tryb przetwarzania zgodnie z obowiązującymi przepisami o ochronie danych osobowych.

- Po zakończeniu realizacji zamówienia Wykonawca zwróci, usunie lub zniszczy dane i nośniki zawierające informacje poufne zgodnie z umową, protokołem odbioru lub odrębnymi instrukcjami Zamawiającego, z wyjątkiem kopii wymaganych przepisami prawa.

Przygotowanie i dostarczenie dokumentacji powykonawczej
Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora.
Dokumentacja techniczna dostarczonego rozwiązania musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści – dla systemów. Powyższe nie dotyczy standardowej dokumentacji producenta sprzętu i oprogramowania a jedynie dokumentacji projektowej.

16.11.2026 r.