OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu wykrywania i reagowania na zagrożenia sieciowe (NDR) wraz z platformą sprzętową i przełącznikiem sieciowym zarządzalnym w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa i wdrożenie dwóch niezależnych, fabrycznie nowych systemów klasy NDR (Network Detection and Response) przeznaczonych do wykrywania i automatycznego reagowania na zagrożenia w sieci IT oraz w sieci OT Zamawiającego, w szczególności ruch boczny (lateral movement), skanowanie portów oraz aktywność oprogramowania ransomware.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Oprogramowanie NDR (licencja) – zgodnie z pkt 1–5 tabeli w rozdz. 3	2 kpl. (1 – sieć IT, 1 – sieć OT)
2.	Platforma sprzętowa NDR (serwer sieciowy) wraz z dyskami SSD – zgodnie z pkt 6–12 tabeli w rozdz. 3	2 szt. (1 – sieć IT, 1 – sieć OT)
3.	Dyski twarde HDD – zgodnie z pkt 11 tabeli w rozdz. 3	min. 2 szt. na każdą platformę (łącznie min. 4 szt.)
4.	Przełącznik sieciowy zarządzalny – zgodnie z pkt 13–16 tabeli w rozdz. 3	2 szt. (1 – sieć IT, 1 – sieć OT)
5.	Usługa wdrożenia systemu NDR w dwóch niezależnych sieciach IT i OT – zgodnie z rozdz. 4	1 usługa

1.3. Oferowane oprogramowanie NDR, platforma sprzętowa, dyski oraz przełącznik muszą stanowić spójne, w pełni współpracujące ze sobą rozwiązanie. W szczególności przełącznik musi być obsługiwany przez oferowane oprogramowanie NDR w zakresie przekazywania pakietów do analizy (pkt 1 i 16 tabeli) oraz automatycznej izolacji hostów na poziomie portu (pkt 4 tabeli), a dyski muszą być obsługiwane przez oferowaną platformę sprzętową.

1.4. Zamówienie obejmuje dostawę dwóch kompletnych zestawów (oprogramowanie NDR, platforma sprzętowa z dyskami, przełącznik) oraz ich wdrożenie: jednego zestawu w sieci IT i jednego zestawu w sieci OT Zamawiającego, zgodnie z rozdz. 4. Zestawy muszą działać jako dwa całkowicie niezależne systemy.

1.5. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 48820000-2 Serwery; 32420000-3 Urządzenia sieciowe; 30233132-5 Napędy dysków twardych; 51612000-5 Usługi instalowania sprzętu do przetwarzania informacji; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Dostarczony sprzęt musi być fabrycznie nowy, nieużywany, nierefabrykowany, nieeksponowany na wystawach, wyprodukowany nie wcześniej niż 12 miesięcy przed dniem dostawy i pochodzić z oficjalnego kanału dystrybucji producenta na rynek Unii Europejskiej.

2.2. Sprzęt musi posiadać oznakowanie CE oraz deklarację zgodności UE, a także spełniać wymagania dyrektywy RoHS.

2.3. Licencja na oprogramowanie NDR musi być udzielona na czas nieoznaczony (bezterminowo), bez ograniczeń czasowych działania funkcji wymienionych w tabeli w rozdz. 3 i bez konieczności ponoszenia przez Zamawiającego opłat cyklicznych. Licencja musi być wystawiona na Zamawiającego.

2.4. Wykonawca zapewni dostęp do aktualizacji oprogramowania NDR (w tym reguł i mechanizmów detekcji) oraz oprogramowania układowego (firmware) platformy i przełącznika przez okres nie krótszy niż okres gwarancji, bez dodatkowych opłat.

2.5. Dyski twarde muszą znajdować się na liście kompatybilności producenta oferowanej platformy sprzętowej, a przełącznik – na liście urządzeń obsługiwanych przez oferowane oprogramowanie NDR (jeżeli producent publikuje takie listy).

2.6. Interfejs zarządzania oprogramowania NDR, platformy sprzętowej i przełącznika musi być dostępny w języku polskim lub angielskim.

2.7. Wynik procesora w teście CPU Mark (pkt 6 tabeli) Zamawiający będzie weryfikował według stanu na stronie https://www.cpubenchmark.net/ na dzień publikacji ogłoszenia. Wykonawca dołączy do oferty wydruk wyniku z tej strony.

2.8. Wraz ze sprzętem Wykonawca dostarczy komplet elementów niezbędnych do jego uruchomienia i montażu, w tym kable zasilające, szyny lub zestawy do montażu w szafie rack 19" oraz dokumentację użytkownika w języku polskim lub angielskim (dopuszcza się wersję elektroniczną).

3. Szczegółowe wymagania techniczne

Oferowane rozwiązanie musi spełniać co najmniej poniższe wymagania minimalne.

Lp.	Parametr	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
Wymagania funkcjonalne dla oprogramowania NDR			
1.	Analiza pakietów	System musi realizować analizę selektywną dedykowanych pakietów sieciowych przekazywanych z przełączników (np. poprzez technologię mirroring/SPAN lub dedykowane API sterujące).	
2.	Model wdrażania	System musi działać jako dedykowana, samodzielna aplikacja/instancja (typu Standalone) instalowana bezpośrednio na posiadanej lub dostarczonej platformie serwerowej pamięci masowej (NAS) bez konieczności dokupowania cyklicznych licencji oprogramowania (model licencjonowania wieczystego lub wbudowanego w ekosystem sprzętowy).	
3.	Analiza behawioralna oparta na sztucznej inteligencji (AI)	System musi wykorzystywać algorytmy uczenia maszynowego i sztucznej inteligencji do stałego monitorowania anomalii w ruchu sieciowym w celu wykrywania ataków typu lateral movement (ruch boczny), skanowania portów oraz infekcji ransomware wewnątrz sieci.	
4.	Automatyczna izolacja (Auto-isolation)	W przypadku wykrycia krytycznego zagrożenia (np. aktywności ransomware) system musi posiadać funkcję automatycznego wydania instrukcji do przełącznika sieciowego w celu natychmiastowego odcięcia/odizolowania zainfekowanego hosta na poziomie portu.	
5.	Scentralizowany panel	Zarządzanie systemem musi odbywać się poprzez responsywny, graficzny interfejs webowy (GUI) umożliwiający szybką weryfikację wektorów ataków oraz topologii sieciowej.	
Platforma sprzętowa NDR (serwer sieciowy)			
6.	Procesor	Architektura x86, minimum 4-rdzeniowy, 4-wątkowy procesor osiągający co najmniej 5000 pkt w teście CPU Mark – https://www.cpubenchmark.net/	
7.	Pamięć operacyjna	Minimum 16 GB pamięci RAM typu DDR5, zainstalowanej w dostarczonym urządzeniu.	
8.	Zatoki na dyski (HDD)	Minimum 4 zatoki formatu 3,5 cala SATA 6 Gb/s z pełnym wsparciem dla technologii Hot-swap (wymiana dysków w trakcie pracy systemu) oraz natywną kompatybilnością z nośnikami 2,5 cala.	
9.	Interfejsy M.2 (SSD)	Minimum 3 gniazda na dyski M.2 2280 PCIe, w tym minimum 2 obsadzone dyskami SSD NVMe o pojemności minimum 500 GB każdy, przeznaczonymi na bazę danych i logi systemu NDR (konfiguracja RAID 1).	

Lp.	Parametr	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
10.	Interfejsy sieciowe	Minimum 2 wbudowane porty miedziane RJ45 o przepustowości minimum 2,5 GbE każdy, wspierające automatyczną negocjację prędkości (2,5G/1G/100M).	
11.	Dyski twarde (HDD)	Minimum 2 sztuki dysków twardych HDD klasy Enterprise lub dedykowanych do systemów NAS pracujących w trybie całodobowym 24/7/365 (np. seria WD Red Pro, Seagate IronWolf Pro lub równoważne). Pojemność pojedynczego dysku: minimum 4 TB.	
12.	Obudowa	Typu RACK 1U z szynami do montażu w szafie RACK.	
Przełącznik sieciowy zarządzalny			
	Producent i model	Należy podać	
13.	Porty miedziane high-speed	Minimum 4 porty 10GbE RJ45 Multi-Gigabit (pełne wsparcie i dopasowanie do prędkości 10G/5G/2.5G/1G/100M).	
14.	Porty światłowodowe	Minimum 8 portów 10GbE SFP+ dedykowanych dla szybkich połączeń szkieletowych i uplink (obsługa modułów SFP+ oraz kabli bezpośredniego połączenia DAC).	
15.	Zarządzanie i funkcje L2	Zarządzanie przez przeglądarkę Web (interfejs graficzny), pełna obsługa standardów: VLAN (802.1Q), agregacja łączy (LACP), IGMP Snooping, mechanizmy zapobiegania pętlom (STP/RSTP). Dedykowany port 1GbE RJ45 do zarządzania przełącznikiem.	
16.	Przechwytywanie ruchu (SPAN)	Pełna i natywna obsługa funkcji Port Mirroring (SPAN) oraz selektywnego kopiowania ruchu (np. mirroring na podstawie reguł ACL) – zdolność kopiowania ruchu wejściowego i wyjściowego z wybranych portów/VLAN-ów, w zakresie wymaganym przez oferowane oprogramowanie NDR, i przesyłania go na dedykowany fizyczny port analityczny spięty z serwerem NDR.	

W celu potwierdzenia zgodności oferowanego rozwiązania z wymaganiami Zamawiający żąda złożenia wraz z ofertą:

- Wypłonionego załącznika nr 2.1 do formularza ofertowego (wskazanie producenta, modelu lub wersji każdego elementu oraz potwierdzenie spełnienia wymagań);
- kart katalogowych lub specyfikacji technicznych producenta dla platformy sprzętowej, dysków i przełącznika;
- dokumentacji producenta oprogramowania NDR (np. karty produktu, instrukcji, listy kompatybilności) potwierdzającej spełnienie wymagań z pkt 1–5 tabeli, w tym obsługę oferowanego przełącznika i oferowanej platformy sprzętowej;
- wydruku wyniku procesora w teście CPU Mark ze strony https://www.cpubenchmark.net/, zgodnie z pkt 2.7.

Jeżeli z dokumentów producenta nie wynika jednoznacznie spełnienie danego wymagania, Wykonawca może złożyć oświadczenie producenta lub jego autoryzowanego przedstawiciela.

4. Wdrożenie w sieciach IT i OT

4.1. Zasady ogólne

4.1.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży jeden kompletny zestaw, obejmujący oprogramowanie NDR, platformę sprzętową z dyskami i przełącznik.

4.1.2. Zestawy dla sieci IT i OT muszą działać całkowicie niezależnie. Zamawiający nie dopuszcza wspólnej konsoli zarządzania, wspólnych kont administracyjnych, synchronizacji konfiguracji ani danych ani jakichkolwiek połączeń sieciowych między zestawami. W trakcie prac Wykonawca nie może zestawiać

połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń, które wcześniej pracowały w sieci IT, bez zgody Zamawiającego.

4.1.3. Interfejsy zarządzania platformy, oprogramowania NDR i przełącznika w każdej sieci muszą być dostępne wyłącznie z wydzielonego segmentu (VLAN) zarządzania danej sieci, wskazanego przez Zamawiającego.

4.1.4. Jeżeli sieć OT nie ma dostępu do Internetu, Wykonawca skonfiguruje zestaw OT do pracy bez połączenia z chmurą producenta i przekaże procedurę aktualizacji w trybie offline (z nośnika lub przez wskazany przez Zamawiającego serwer pośredniczący).

4.1.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym.

4.2. Analiza przedwdrożeniowa i projekt techniczny

4.2.1. W terminie do 14 dni od zawarcia umowy Wykonawca przeprowadzi, wspólnie z Zamawiającym, analizę przedwdrożeniową każdej sieci, obejmującą co najmniej: segmenty i sieci VLAN objęte monitorowaniem, punkty włączenia przełącznika NDR w istniejącą infrastrukturę, adresację, segment zarządzania oraz listę urządzeń krytycznych.

4.2.2. Na podstawie analizy Wykonawca opracuje odrębny projekt techniczny wdrożenia dla sieci IT i dla sieci OT, zawierający schemat połączeń, adresację, konfigurację przełącznika, zakres przekazywania ruchu do analizy, polityki reagowania oraz harmonogram prac. Prace instalacyjne mogą rozpocząć się po akceptacji projektu przez Zamawiającego.

4.3. Zakres prac w każdej sieci

- montaż platformy sprzętowej i przełącznika w szafie rack wskazanej przez Zamawiającego, podłączenie zasilania (w tym do zasilania gwarantowanego UPS, jeżeli jest dostępne) i okablowania krosowego oraz trwałe oznakowanie urządzeń i przewodów;
- instalacja dysków, konfiguracja macierzy RAID 1 dla dysków HDD oraz dla dysków SSD przeznaczonych na bazę danych i logi systemu NDR;
- aktualizacja systemu operacyjnego platformy, oprogramowania NDR i oprogramowania układowego przełącznika do najnowszych wersji udostępnionych przez producenta;
- utwardzenie konfiguracji (hardening): zmiana wszystkich domyślnych haseł, wyłączenie zbędnych usług i protokołów, dostęp administracyjny wyłącznie przez HTTPS/SSH z segmentu zarządzania, imienne konta administratorów z podziałem uprawnień, uwierzytelnianie wieloskładnikowe (jeżeli jest obsługiwane), synchronizacja czasu z serwerem NTP wskazanym przez Zamawiającego;
- konfiguracja przełącznika: sieci VLAN, port analityczny, przekazywanie ruchu do analizy (SPAN lub mirroring selektywny), integracja z oprogramowaniem NDR w zakresie izolacji portów oraz włączenie przełącznika w istniejącą infrastrukturę sieciową zgodnie z projektem;
- instalacja i konfiguracja oprogramowania NDR: rejestracja przełącznika, inwentaryzacja wykrytych urządzeń, konfiguracja mechanizmów wabików (honeypot/threat trap) – jeżeli rozwiązanie je udostępnia, polityk ochrony, list wyjątków oraz powiadomień (e-mail i syslog do systemu wskazanego przez Zamawiającego, np. SIEM);
- wykonanie kopii zapasowej konfiguracji wszystkich urządzeń po zakończeniu wdrożenia i przekazanie jej Zamawiającemu.

4.4. Polityki reagowania

4.4.1. Po uruchomieniu systemu w każdej sieci Wykonawca przeprowadzi okres obserwacji i strojenia reguł trwający nie krócej niż 14 dni, w celu ograniczenia fałszywych alarmów. Automatyczną izolację można włączyć dopiero po zakończeniu tego okresu.

4.4.2. Sieć IT: system będzie automatycznie izolował hosty, dla których wykryto zagrożenia o wysokim lub krytycznym poziomie ryzyka. Urządzenia infrastrukturalne wskazane przez Zamawiającego (np. serwery, kontrolery domeny, urządzenia sieciowe) zostaną objęte listą wyjątków lub trybem wymagającym potwierdzenia administratora.

4.4.3. Sieć OT: domyślnie system będzie pracował w trybie monitorowania i powiadamiania, bez automatycznej izolacji. Automatyczną izolację można włączyć wyłącznie dla urządzeń wskazanych przez Zamawiającego na piśmie. Urządzenia sterowania procesem (m.in. sterowniki PLC, RTU, serwery SCADA, stacje HMI) muszą zostać wyłączone z automatycznej izolacji.

4.4.4. W obu sieciach administrator musi mieć możliwość ręcznego cofnięcia izolacji z poziomu konsoli NDR.

4.5. Testy odbiorowe

Wykonawca przeprowadzi w każdej sieci testy według scenariusza zaakceptowanego przez Zamawiającego, z użyciem własnego hosta testowego i nieszkodliwych narzędzi (bez użycia rzeczywistego złośliwego oprogramowania). Testy obejmą co najmniej:

- potwierdzenie poprawnego przekazywania ruchu z przełącznika do analizy;
- wykrycie symulowanego skanowania portów z hosta testowego;
- wykrycie symulowanej próby ruchu bocznego (np. prób logowania SMB/SSH do innego hosta lub wabika);
- w sieci IT – automatyczną izolację hosta testowego na poziomie portu przełącznika i jej ręczne cofnięcie;
- w sieci OT – wygenerowanie alertu bez izolacji hosta oraz ręczną izolację i cofnięcie izolacji hosta testowego;
- dostarczenie powiadomień e-mail i komunikatów syslog do wskazanego systemu;
- brak dostępu do interfejsów zarządzania spoza segmentu zarządzania oraz brak połączeń między zestawami IT i OT.

4.6. Dokumentacja i instruktaż

4.6.1. Wykonawca przekaże w języku polskim odrębną dokumentację powykonawczą dla sieci IT i dla sieci OT, obejmującą co najmniej: schemat połączeń, adresację, wyeksportowane konfiguracje urządzeń, wykaz kont, opis polityk reagowania i list wyjątków, protokoły z testów oraz procedury: obsługi alertu, cofnięcia izolacji, aktualizacji (dla sieci OT – również w trybie offline), wymiany dysku oraz odtworzenia konfiguracji. Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

4.6.2. Wykonawca przeprowadzi w siedzibie Zamawiającego instruktaż dla administratorów w wymiarze nie mniejszym niż **4** godzin dla maksymalnie **2** osób, obejmujący obsługę obu zestawów, analizę zdarzeń, zarządzanie politykami i izolacją oraz procedury z pkt 4.6.1.

4.6.3. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT.

5. Gwarancja i serwis

5.1. Wykonawca udzieli gwarancji na cały przedmiot zamówienia, w tym na prawidłowe działanie wykonanej konfiguracji, na okres nie krótszy niż **24** miesięcy, liczony od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń.

5.2. Gwarancja musi być realizowana przez producenta lub autoryzowanego partnera serwisowego producenta na terenie Polski. Zgłoszenia przyjmowane są w dni robocze, telefonicznie, e-mailem lub przez portal serwisowy.

5.3. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych. Czas naprawy lub wymiany urządzenia na wolne od wad: nie dłuższy niż **3** dni roboczych od zgłoszenia. Po wymianie urządzenia Wykonawca odtworzy jego konfigurację.

5.4. Uszkodzone nośniki danych (dyski HDD oraz SSD) pozostają u Zamawiającego i nie podlegają zwrotowi do Wykonawcy ani producenta, bez utraty uprawnień gwarancyjnych.

5.5. Koszty transportu sprzętu w ramach gwarancji ponosi Wykonawca.

6. Termin, miejsce realizacji i odbiór

6.1. Termin dostawy: do **20** dni od dnia zawarcia umowy. Termin zakończenia wdrożenia w obu sieciach (łącznie z okresem obserwacji z pkt 4.4.1 i testami odbiorowymi): do **20** dni od dnia zawarcia umowy.

6.2. Miejsce realizacji: Siedziba zamawiającego. Dostawa odbywa się na koszt i ryzyko Wykonawcy, w dni robocze w godzinach **8:00-16:00**, po wcześniejszym uzgodnieniu terminu z Zamawiającym.

6.3. Odbiór dostawy nastąpi na podstawie protokołu odbioru ilościowo-jakościowego, po sprawdzeniu kompletności dostawy i zgodności z ofertą. Wraz z dostawą Wykonawca przekaże dokumenty licencyjne oraz dokumenty gwarancyjne.

6.4. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 4.5 oraz przekazaniu dokumentacji z pkt 4.6.1. Po odbiorze wdrożenia w obu sieciach i przeprowadzeniu instruktażu strony podpiszą protokół odbioru końcowego.

7. Rozwiązania równoważne

7.1. Wskazane w opisie przedmiotu zamówienia nazwy własne, znaki towarowe, normy lub pochodzenie (w tym przykładowe serie dysków w pkt 11 tabeli) mają charakter przykładowy i służą wyłącznie określeniu wymaganego standardu jakościowego i funkcjonalnego. Zamawiający dopuszcza rozwiązania równoważne.

7.2. Za rozwiązanie równoważne Zamawiający uzna rozwiązanie o parametrach technicznych, funkcjonalnych i jakościowych nie gorszych niż wymagane w niniejszym OPZ. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.