OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu NDR (Network Detection &and Response)

1. Przedmiot zamówienia

1.1. Zakres

Przedmiotem zamówienia jest dostawa, instalacja, wdrożenie, konfiguracja i integracja z infrastrukturą Zamawiającego systemu klasy Network Detection and Response (NDR), wraz z licencjami i subskrypcjami, Optymalizacją, testami odbiorczymi, szkoleniami, dokumentacją oraz wsparciem technicznym i aktualizacjami w Okresie wsparcia (pkt 2.3, A.08, U.01).

System ma monitorować ruch sieciowy, wykrywać anomalie i zagrożenia oraz reagować na nie w infrastrukturze IT oraz w ruchu OT/ICS/IoT widocznym w punktach zbierania ruchu (pkt 3.1), z wykorzystaniem analizy behawioralnej opartej na uczeniu maszynowym (ML) lub sztucznej inteligencji (AI) (F.08).

1.2. Kontekst wymagań

Zamawiający jest przedsiębiorstwem wodociągowo-kanalizacyjnym, zaliczonym do podmiotów ważnych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Na kształt wymagań wpływają w szczególności: nadmiarowe punkty agregacji ruchu (pkt 3.1); terminy zgłaszania incydentów poważnych wynikające z ustawy o krajowym systemie cyberbezpieczeństwa, wymagające szybkiego dostępu do materiału dowodowego, a więc lokalnej retencji danych; posiadana zapora NGFW jako jedyny punkt egzekucji polityk bezpieczeństwa, na którym ma być realizowana aktywna reakcja w zakresie ruchu przechodzącego przez zaporę (pkt 6.9).

Dominującym scenariuszem zagrożenia jest ransomware: kompromitacja stacji roboczej, ruch boczny (głównie SMB) i masowe szyfrowanie zasobów plikowych, w najgorszym wariancie z przeniesieniem na OT. Jego wykrycie wymaga obserwacji przebiegu komunikacji i plików przenoszonych w ruchu, a ocena zasięgu incydentu – retrospektywnego ustalenia, gdzie w sieci wystąpił dany plik lub wskaźnik (pkt 5.2).

1.3. Cena i rozliczenie

Cena oferty obejmuje całość przedmiotu zamówienia: dostawę sprzętu, licencji i subskrypcji wraz ze wsparciem producenta i Wykonawcy w Okresie wsparcia, Wdrożenie oraz Optymalizację.

Wynagrodzenie płatne jest na podstawie jednej faktury, wystawionej po podpisaniu protokołu odbioru wdrożenia (pkt 9.4). Wynagrodzenie za Optymalizację jest zawarte w cenie oferty; protokół zakończenia Optymalizacji (pkt 9.5) nie stanowi podstawy do odrębnego wynagrodzenia. Termin płatności, skutki opóźnienia oraz pozostałe warunki rozliczenia określa wzór umowy.

2. Zasady ogólne

2.1. Charakter wymagań i sposób wykazania zgodności

Wymagania rozdziałów 4–6 są obligatoryjne; oferta niespełniająca któregokolwiek z nich podlega odrzuceniu. Zamawiający nie stosuje wymagań fakultatywnych ani punktowanych za funkcje produktu. Parametry wydajnościowe i pojemnościowe są wartościami minimalnymi, a parametry czasowe, wysokość obudowy, pobór mocy oraz limity zasobów platformy wirtualizacyjnej (pkt 3.1) – wartościami maksymalnymi. Rozwiązania o parametrach lepszych są dopuszczalne.

Spełnienie wymagań rozdziałów 4–6 Wykonawca wykazuje przedmiotowymi środkami dowodowymi wskazanymi w Dokumentach zamówienia z odesłaniem do publicznie dostępnej dokumentacji producenta. Wykonawca składa: karty katalogowe oferowanych komponentów fizycznych, wykaz zasobów maszyn wirtualnych (A.06), wskazanie publikacji potwierdzającej zgodność integracyjną z zaporą (F.38), wykaz lokalizacji przetwarzania danych (F.50) oraz opis działania Systemu po wygaśnięciu subskrypcji (A.08).

Rozdziały 7–12 oraz Załącznik nr 1 określają obowiązki Wykonawcy w trakcie realizacji umowy.

2.2. Nazwy własne, normy i równoważność

Standardy i formaty wymienione jako przykład realizacji funkcji (JA3/JA4, STIX/TAXII, MITRE ATT&CK) należy czytać z dopiskiem „lub równoważne". Nie dotyczy to protokołów i formatów wynikających ze środowiska Zamawiającego (rozdział 3, F.22, F.30), których obsługa jest obligatoryjna. Równoważne jest rozwiązanie dające ten sam efekt w zakresie nie mniejszym niż opisany, bez obniżenia parametrów i bez dodatkowych kosztów po stronie Zamawiającego; ciężar wykazania równoważności spoczywa na Wykonawcy, a oświadczenie bez potwierdzenia w dokumentacji technicznej nie wystarcza.

Posiadana infrastruktura, w szczególności zapora sieciowa, opisuje środowisko współpracy i nie podlega zastąpieniu rozwiązaniem równoważnym; system NDR nie musi pochodzić od producenta zapory – wymagana jest potwierdzona zgodność integracyjna (F.38).

2.3. Definicje

Pojęcie	Znaczenie
Dokumenty zamówienia	specyfikacja warunków zamówienia wraz z załącznikami, w tym wzorem umowy i formularzem cenowym.
System	Oferowany system NDR wraz ze wszystkimi komponentami, licencjami i subskrypcjami.
Sonda	Komponent (fizyczny lub wirtualny) podłączony do łączy monitorujących, realizujący przechwytywanie i analizę ruchu.
Konsola	Komponent (fizyczny lub wirtualny) realizujący zarządzanie, przechowywanie danych, wyszukiwanie, raportowanie i integracje (kolektor—/, konsola centralna). W rozwiązaniu jednoelementowym funkcje sondy i konsoli realizuje ten sam komponent.
Komponent fizyczny	Komponent dostarczany wraz ze sprzętem, na którym pracuje: urządzenie fizyczne albo oprogramowanie na dedykowanej platformie sprzętowej dostarczonej przez Wykonawcę (A.01 lit. a i b), także gdy działa na niej w maszynie wirtualnej.
Komponent wirtualny	Komponent dostarczany jako obraz maszyny wirtualnej producenta (virtual appliance), uruchamiany na platformie wirtualizacyjnej Zamawiającego (A.01 lit. c, A.05–A.06).
Punkt zbierania ruchu	Jeden z dwóch punktów agregacji ruchu opisanych w pkt 3.1: rdzeń sieci IT albo sieć centrum danych.
Łącze monitorujące	Łącze 10GbE SFP+ od portu docelowego sesji lustrzanej (SPAN) na przełączniku Zamawiającego do interfejsu monitorującego Systemu; łącznie cztery łącza opisane w pkt 3.2.

Pojęcie	Znaczenie
IoC	Wskaźnik kompromitacji: adres IP, domena, URL, suma kontrolna pliku (SHA-256, SHA-1 lub MD5).
Metadane sieciowe	Przeszukiwalne rekordy opisujące sesje i przepływy wraz z ich wzbogaceniem; nie obejmują pełnej treści pakietów.
Pojemność użytkowa	Pojemność przestrzeni dyskowej dostępna dla danych Systemu po uwzględnieniu narzutu konfiguracji nadmiarowej; dla komponentów wirtualnych – pojemność przydzielonych im dysków wirtualnych; w architekturze rozproszonej lub mieszanej – suma dla wszystkich komponentów.
Brak utraty pakietów	Stan, w którym w każdym interwale 1 min, w którym łączny ruch na łączach monitorujących (według liczników portów docelowych sesji lustrzanych, odczytywanych przez Zamawiającego co 1 min, przed deduplikacją) nie przekracza wartości z T.01, liczba pakietów odrzuconych przez System z powodu braku zasobów (liczniki odrzuceń interfejsów, buforów przechwytywania i kolejek silników analitycznych, udostępniane przez Wykonawcę w tym samym interwale) nie przekracza 0,1 % pakietów odebranych. Utratą nie jest udokumentowane w ofercie pomijanie analizy części sesji (np. limit głębokości analizy sesji), jeżeli nie ogranicza ono wymagań F.18 i T.02.
Fałszywy alarm	Alarm, którego przesłanki (F.10) nie odpowiadają rzeczywistemu stanowi ruchu. Alarm prawidłowo opisujący ruch, który Zamawiający uznaje za dozwolony, nie jest fałszywym alarmem; jego wyciszenie jest działaniem strojącym (F.32).
Wdrożenie	Instalacja i uruchomienie produkcyjne Systemu, w którym System odbiera i analizuje ruch ze wszystkich punktów zbierania, przekazuje zdarzenia do systemu zbierania logów, jest zintegrowany kompatybilnie z funkcjonującą u Zamawiającego NGFW, a funkcje objęte scenariuszami części A Programu testów działają, co potwierdza test akceptacyjny; funkcje wymagające okresu nauki są uruchomione w trybie nauki. Pozostałe funkcje rozdziału 6 są dostępne w Systemie; ich konfigurację docelową, w tym zasady automatycznej reakcji, wykonuje się i weryfikuje w Optymalizacji.
Odbiór wdrożenia	Podpisanie protokołu odbioru wdrożenia (pkt 9.4), potwierdzającego Wdrożenie oraz dostawę sprzętu, licencji i subskrypcji, z podaniem ich ilości i okresu ważności. Podpisany protokół stanowi podstawę do wystawienia faktury (pkt 1.3).
Optymalizacja	Etap realizacji zamówienia następujący po Odbiorze wdrożenia, obejmujący prace z pkt 7.2 i zakończony podpisaniem protokołu zakończenia Optymalizacji (pkt 9.5) w terminie z rozdziału 8. Wynagrodzenie za Optymalizację jest zawarte w cenie oferty (pkt 1.3).
Okres wsparcia	Nie krótszy niż 36 miesięcy liczony od dnia podpisania Protokołu Odbioru Wdrożenia.
Program testów	Program testów odbiorczych stanowiący Załącznik nr 1, z uszczegółowieniem uzgodnionym w projekcie technicznym (pkt 9.1).

Pojęcie	Znaczenie
Okno serwisowe	Uzgodniony przez Strony przedział czasu przeznaczony na prace ingerujące w konfigurację sieci produkcyjnej, zapory lub platformy wirtualizacyjnej Zamawiającego (pkt 7.3).
Dzień roboczy	Dzień od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy.
Godziny robocze	Godziny 8:00–16:00 w dni robocze.
NBD	Dostarczenie i instalacja sprzętu zastępczego następnego dnia roboczego po dniu zgłoszenia, jeżeli zgłoszenie zarejestrowano do godz. 16:00; zgłoszenie zarejestrowane później traktuje się jak zarejestrowane następnego dnia roboczego.

3. Środowisko Zamawiającego

3.1. Infrastruktura i usługi

Element	Dane istotne dla doboru rozwiązania
Zapora sieciowa (NGFW)	Fortinet FortiGate 120G w klastrze HA w trybie active-passive. FortiOS v7.4.13 – jedyny punkt egzekucji polityk bezpieczeństwa na styku sieci. Przez zaporę przechodzi ruch z Internetem oraz między segmentami.
Systemy towarzyszące zaporze	FortiAnalyzer (maszyna wirtualna), wolumen 5 GB/dobę. Zamawiający nie eksploatuje systemu centralnego zarządzania konfiguracją zapory (FortiManager). Odnowienie posiadanych licencji i subskrypcji w okresie umowy leży po stronie Zamawiającego.
Punkty zbierania ruchu	Dwa niezależne, nadmiarowe punkty agregacji: rdzeń sieci IT oraz sieć centrum danych. Do każdego punktu prowadzą dwa odrębne łącza monitorujące z dwóch przełączników, tak aby awaria lub restart pojedynczego przełącznika nie powodowały utraty widoczności – łącznie 4 jednoczesne łącza 10GbE SFP+ (pkt 3.2). Liczba i rodzaj łączy wynikają z topologii, a nie z wolumenu ruchu; wymaganą przepustowość analizy określa T.01.
Zakres lustrzenia	Sieci VLAN z komunikacją użytkowników, serwerów i systemów aplikacyjnych, w relacji północ–południe i wschód–zachód, z wyłączeniem sieci pamięci masowej oraz sieci VLAN OT.
Sesje lustrzane	Sesje lustrzane (SPAN) dla czterech łączy monitorujących są skonfigurowane przez Zamawiającego według jego projektu (źródłowe sieci VLAN według zakresu lustrzenia, porty docelowe według pkt 3.2) i aktywne w dniu wszczęcia postępowania. Wykonawca weryfikuje ich poprawność w analizie przedwdrożeniowej (pkt 7.1); zmiany wynikające z weryfikacji wprowadza Zamawiający (pkt 7.3).
IPv6	W sieci objętej monitorowaniem IPv6 nie występuje.

Element	Dane istotne dla doboru rozwiązania
Segment OT	Obiekty rozproszone; urządzenia OT komunikują się z centralą przez prywatny APN (połączenia routowane). Protokoły przemysłowe używane w sieci Zamawiającego: Modbus/TCP, OPC UA, PROFINET, EtherNet/IP. Protokoły przemysłowe widoczne w punktach zbierania ruchu, tj. przenoszone w sieciach VLAN objętych zakresem lustrzenia (F.22): Modbus/TCP, OPC UA, PROFINET, EtherNet/IP.
Platforma wirtualizacyjna	Proxmox Virtual Environment. Na potrzeby komponentów wirtualnych Zamawiający może przydzielić łącznie nie więcej niż: 64 vCPU, 256 GB RAM, 40 TB przestrzeni dyskowej na nośnikach HDD w konfiguracji RAIDZ2 oraz 4 portów fizycznych 10GbE SFP+ z obsługą SR-IOV. Infrastruktura wykorzystuje dysk NVMe SSD o pojemności nominalnej 400 GB, przeznaczony do obsługi mechanizmów przyspieszających pracę ZFS. Rozwiązanie wymagające zasobów większych niż powyższe dostarcza dla odpowiedniej części Systemu komponent fizyczny.
Skala środowiska (stan na dzień wszczęcia postępowania)	150 hostów i urządzeń końcowych; 50 maszyn wirtualnych i serwerów (Windows Server, Linux); 200 kamer monitoringu wizyjnego; 20 przełączników Cisco; 200 czujników i urządzeń OT komunikujących się przez prywatny APN; system EDR (integracja Systemu z EDR nie jest wymagana); systemy dziedzinowe wspierające działalność wodociągowo-kanalizacyjną.
Miejsce instalacji	Szafa RACK 19"; dostępna przestrzeń, zasilanie i chłodzenie pozwalają na instalację komponentów fizycznych o łącznej wysokości do 4U i łącznym maksymalnym poborze mocy do 1500 W (T.09), zasilanych z dwóch niezależnych obwodów; listwy zasilające z gniazdami C13 (IEC 60320).
Usługi współpracujące	Active Directory (uwierzytelnianie konsoli i wzbogacanie zdarzeń); dostęp przez LDAPS (lub LDAP z StartTLS); Microsoft Entra ID (dostawca tożsamości, możliwy do wykorzystania dla MFA – F.44); serwer SNMP (SNMPv3); system zbierania logów (centralne logowanie, odbiór zdarzeń syslog); serwer NTP Zamawiającego.
Zewnętrzna usługa SOC/MDR	Zamawiający korzysta z zewnętrznej usługi SOC/MDR. Konfiguracja odbioru po stronie operatora SOC nie należy do Wykonawcy.

Szczegółowe dane konfiguracyjne adresacja, podział na sieci VLAN, parametry kont serwisowych, adresy usług) zostaną przekazane wybranemu Wykonawcy na etapie analizy przedwdrożeniowej.

3.2. Łącza monitorujące

Tabela 3.2. Parametry łączy monitorujących

Łącze	Punkt zbierania	Przełącznik źródłowy: platforma, typ portu docelowego	Odległość do miejsca instalacji (trasa kablowa)	Medium i złącza po stronie przełącznika
L1	Rdzeń sieci IT – przełącznik 1	platforma Cisco 10GbE	1m	SFP+
L2	Rdzeń sieci IT – przełącznik 2	platforma Cisco 10GbE	1m	SFP+

Łącze	Punkt zbierania	Przełącznik źródłowy: platforma, typ portu docelowego	Odległość do miejsca instalacji (trasa kablowa)	Medium i złącza po stronie przełącznika
L3	Centrum danych – przełącznik 1	platforma NEXUS 10/25 GbE	5m	SFP28/ SFP+
L4	Centrum danych – przełącznik 2	platforma NEXUS 10/25 GbE	5m	SFP28/ SFP+

3.3. Założenia do wyceny

Zamawiający nie dysponuje pełną charakterystyką ruchu w punktach zbierania. Do wyceny i doboru rozwiązania oraz do oceny spełnienia T.01, T.07 i A.09 przyjmuje się następujące założenia:

a) łączny ruch na łączach monitorujących – do 5 Gb/s (średnia w każdym 1-minutowym interwale), według liczników portów docelowych sesji lustrzanych, przed deduplikacją;

b) liczba unikalnych adresów IP z sieci wewnętrznych widocznych w ruchu – do 1 000;

c) średni dobowy wolumen ruchu na łączach monitorujących, przed deduplikacją – do 12 TB na dobę;

d) średnia dobowa liczba nowych sesji – do 200 na sekundę.

4. Architektura, forma dostawy i licencje

Nr	Wymaganie
A.01	**Forma realizacji.** System realizuje wszystkie funkcje wymagane w rozdziałach 5–6 jako pojedynczy komponent albo w architekturze rozproszonej (co najmniej jedna sonda i konsola). Zamawiający nie narzuca liczby komponentów ani podziału funkcji pomiędzy nie. Każdy komponent może zostać dostarczony jako: a) urządzenie fizyczne; b) oprogramowanie wraz z dedykowaną platformą sprzętową dostarczoną przez Wykonawcę w cenie oferty i objętą wsparciem producenta – także w postaci maszyny wirtualnej uruchamianej na tej platformie, przy czym warstwa wirtualizacji wraz z licencją i wsparciem na Okres wsparcia stanowi wówczas część dostawy; c) maszyna wirtualna uruchamiana na platformie wirtualizacyjnej Zamawiającego, na warunkach A.05–A.06. Formy a)-–c) mogą być łączone w ramach jednego rozwiązania (forma mieszana).
A.02	**Jeden producent.** Oprogramowanie wszystkich komponentów funkcjonalnych (sondy, konsola, silniki analityczne) pochodzi od jednego producenta systemu NDR, jest objęte jedną ceną oferty i jednym wsparciem producenta; platforma sprzętowa i warstwa wirtualizacji – zgodnie z A.01 lit. b i A.04. Funkcje dla środowisk IT i OT mogą być realizowane przez moduły tego producenta; dopuszcza się odrębne interfejsy modułów pod warunkiem wspólnego uwierzytelniania (SSO), wspólnej listy zdarzeń w konsoli głównej i jednego wsparcia producenta.

Nr	Wymaganie
A.03	**Samowystarczalność.** Wszystkie komponenty niezbędne do spełnienia wymagań dostarczane są w ramach zamówienia i objęte ceną oferty, bez dodatkowych kosztów licencyjnych, sprzętowych lub wirtualizacyjnych po stronie Zamawiającego. Poza komponentami wirtualnymi (A.05–A.06) żaden komponent nie jest uruchamiany na zasobach Zamawiającego (macierz dyskowa, serwery), a rozwiązanie nie wymaga instalacji agentów na serwerach, stacjach roboczych ani urządzeniach automatyki. Żaden komponent realizujący wymagane funkcje nie może być usługą chmurową; dopuszczalne wyjątki – uzupełniająca weryfikacja reputacji plików i sum kontrolnych oraz uzupełniająca analiza dynamiczna (F.19), realizowane na terenie EOG, oraz pobieranie aktualizacji i wskaźników (F.14, F.15, F.49) – nie mogą być warunkiem pracy Systemu.
A.04	**Sprzęt.** Cały dostarczany sprzęt jest fabrycznie nowy, nieużywany, nieregenerowany, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostawy, pochodzi z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej i jest przystosowany do montażu w szafie 19". Dopuszcza się platformę sprzętową producenta oferowanego systemu albo platformę certyfikowaną przez tego producenta i objętą jego wsparciem. Przy dostawie Wykonawca potwierdza spełnienie wymagania rejestracją numerów seryjnych na portalu producenta na Zamawiającego jako użytkownika końcowego (A.08), a datę produkcji – oznaczeniem na urządzeniu lub informacją z portalu producenta.
A.05	**Komponent wirtualny.** Komponent wirtualny dostarczany jest jako obraz maszyny wirtualnej (virtual appliance) stanowiący standardowy produkt producenta oferowanego systemu, objęty przez cały Okres wsparcia wsparciem tego producenta dla Proxmox VE w wersji wskazanej w pkt 3.1 albo dla KVM/QEMU z urządzeniami virtio w wersji zgodnej z tą platformą. Uruchomienie komponentu na platformie Zamawiającego leży po stronie Wykonawcy. Licencja nie jest powiązana z identyfikatorem sprzętowym hosta w sposób uniemożliwiający przeniesienie maszyny wirtualnej na inny host lub jej odtworzenie z kopii zapasowej; operacje te nie wymagają udziału producenta ani zakupu nowej licencji.
A.06	**Zasoby komponentów wirtualnych.** Wykonawca wskazuje w ofercie zasoby wymagane dla każdej maszyny wirtualnej (Punkt 3.3 formularza ofertowego tj. Komponenty w formie c) – zasoby i porty (A.06, T.10 OPZ) – jeżeli dotyczy) zgodne z dokumentacją producenta i wystarczające do spełnienia wszystkich wymagań rozdziału 5: vCPU, RAM, przestrzeń dyskową, wymagane rezerwacje, wymagane rozszerzenia zestawu instrukcji procesora (np. AVX2) i ustawienie typu procesora maszyny wirtualnej w Proxmox VE, minimalną wydajność przydzielonej przestrzeni dyskowej (IOPS, przepustowość, opóźnienie, wraz z profilem operacji), wymagania dotyczące NUMA i pamięci hugepages – jeżeli występują – oraz liczbę i sposób podłączenia interfejsów. Łączne zasoby i parametry wskazane w ofercie nie mogą przekraczać limitów określonych w pkt 3.1 ani wymagać rozszerzeń procesora, których nie zapewniają wskazane tam procesory hostów; jeżeli rozwiązanie wymaga zasobów większych, Wykonawca dostarcza dla odpowiedniej części Systemu komponent fizyczny. Zasoby wskazane w ofercie są wiążące dla Wykonawcy. Rozwiązanie nie wymaga od Zamawiającego zakupu dodatkowych licencji platformy wirtualizacyjnej, zmiany jej wersji lub edycji ani rozbudowy sprzętowej hostów (z zastrzeżeniem T.10 w zakresie portów). Licencje systemów operacyjnych, baz danych i innego oprogramowania uruchamianego w maszynach wirtualnych Wykonawca zapewnia w cenie oferty.

Nr	Wymaganie
A.07	**Niezależność od formy dostawy.** Wymagania wydajnościowe, pojemnościowe i funkcjonalne obowiązują bez względu na formę dostawy; dla komponentów wirtualnych ich spełnienie weryfikowane jest w testach odbiorczych przy zasobach nie większych niż wskazane w ofercie (A.06). Wymagania dotyczące obudowy, zasilania, nośników i wymiany sprzętu (A.04, T.09, U.03) dotyczą komponentów fizycznych.
A.08	**Licencja i wsparcie producenta.** Licencja/subskrypcja i wsparcie producenta ważne przez cały Okres trwania umowy 36 miesięcy od dnia podpisania Protokołu Odbioru Wdrożenia, obejmujące prawo do korzystania ze wszystkich funkcji wymaganych w rozdziałach 5–6 (w tym modułów analizy złośliwego oprogramowania) oraz aktualizacje oprogramowania, sygnatur, modeli analitycznych i baz reputacyjnych. Jeżeli producent liczy okres licencji/subskrypcji od daty dostawy, aktywacji lub rejestracji, Wykonawca zapewnia w cenie oferty licencję/subskrypcję o okresie odpowiednio dłuższym. Licencje i subskrypcje umożliwiają pracę Systemu od jego uruchomienia, także przed Odbiorem wdrożenia. Wsparcie producenta jest zarejestrowane na Zamawiającego jako użytkownika końcowego, z możliwością samodzielnej weryfikacji statusu na portalu producenta. Wykonawca wskazuje w ofercie zakres działania Systemu po wygaśnięciu subskrypcji. Na koniec Okresu wsparcia System umożliwia eksport zdarzeń, metadanych i konfiguracji w formacie maszynowo przetwarzalnym.
A.09	**Zakres licencji i rozbudowa.** Licencja nie ogranicza liczby użytkowników konsoli, ról, reguł, wyjątków, raportów ani sieci VLAN. Jeżeli model licencyjny producenta zawiera limit hostów (unikalnych adresów IP lub urządzeń), Wykonawca dostarcza licencję o limicie nie niższym niż 1 500, tj. 150 % liczby z pkt 3.3 lit. b, bez konieczności rozszerzania jej w Okresie wsparcia. Realizacja integracji opisanych w pkt 6.9 oraz w rozdziale 7 nie wymaga zakupu dodatkowych licencji, modułów ani subskrypcji. Rozbudowa Systemu o 2 dodatkowe sondy o łącznej przepustowości do 1 Gb/s nie może wymagać wymiany dostarczonych komponentów ani zakupu licencji innej niż licencja dodawanej sondy.

5. Wymagania wydajnościowe, pojemnościowe i sprzętowe

5.1. Wydajność

Nr	Wymaganie
T.01	**Przepustowość.** Przepustowość analizowanego ruchu co najmniej 5 Gb/s łącznie z czterech jednocześnie pracujących łączy monitorujących w architekturze rozproszonej łącznie ze wszystkich sond – mierzona jako średnia w interwale 1 min, przed deduplikacją, według liczników portów docelowych sesji lustrzanych, przy jednoczesnej pracy wszystkich wymaganych modułów analitycznych, także w czasie wyszukiwania retrospektywnego i generowania raportów, przy obsłudze wszystkich aktywnych hostów widocznych w monitorowanym ruchu i przy profilu ruchu odpowiadającym ruchowi rzeczywistemu Zamawiającego-, bez utraty pakietów w rozumieniu pkt 2.3. Spełnienie wymagania weryfikuje się testem 72-godzinnym na ruchu rzeczywistym i testem obciążeniowym 1-godzinnym (Załącznik nr 1).

5.2. Retrospektywne ustalanie zasięgu incydentu

System ma umożliwiać ustalenie po fakcie, gdzie w monitorowanej sieci wystąpił plik lub wskaźnik uznany za złośliwy – w celu oceny zasięgu incydentu w terminach zgłaszania incydentów poważnych wynikających z ustawy o krajowym systemie cyberbezpieczeństwa – wyłącznie na podstawie danych zgromadzonych z analizy ruchu, bez skanowania zasobów plikowych, bez dostępu do udziałów sieciowych i bez instalowania komponentów na serwerze plików.

Nr	Wymaganie
T.02	**Sumy kontrolne plików.** Wyznaczanie sum kontrolnych SHA-256, SHA-1 i MD5 każdego pliku wyodrębnionego z ruchu (F.18), z powiązaniem każdego wystąpienia z sesją, hostem źródłowym i docelowym, protokołem, kierunkiem transferu i znacznikiem czasu; dane przechowywane przez cały okres retencji metadanych (T.07). Wymaganie dotyczy plików przesłanych w całości, o rozmiarze do 50 MB, następujących typów: pliki wykonywalne (w tym PE i ELF), skrypty, dokumenty biurowe (w tym z makrami), pliki PDF i archiwa; dla transferów niepełnych System odnotowuje transfer częściowy.
T.03	**Wyszukiwanie po sumie kontrolnej.** Wyszukanie po sumie kontrolnej w pełnym zakresie retencji w czasie nie dłuższym niż 5 minut, zwracające listę wszystkich wystąpień pliku w ruchu z danymi z T.02 oraz listę hostów, które wysłały lub odebrały plik, z możliwością przejścia do karty zdarzenia i widoku analizy powłamaniowej (F.07); wynik eksportowalny (F.28) i dostępny przez REST API.
T.04	**Automatyczne przeszukanie wsteczne.** Automatyczne przeszukanie zgromadzonych danych historycznych po dodaniu nowego IoC – wprowadzonego ręcznie, zaimportowanego lub pobranego ze źródła zewnętrznego – z wygenerowaniem zdarzenia dla trafień historycznych. Operacje z T.03 i T.04 nie powodują utraty pakietów ani obniżenia przepustowości poniżej T.01.

5.3. Pojemność i przechowywanie danych

Nr	Wymaganie
T.05	**Przestrzeń dyskowa.** Lokalna przestrzeń dyskowa w konfiguracji nadmiarowej odpornej na awarię co najmniej jednego nośnika (RAID 1/5/6/10 lub równoważnej), z nośnikami wymiennymi podczas pracy, o łącznej pojemności użytkowej co najmniej 7 TB, a w każdym przypadku wystarczającej do spełnienia T.07 przy założeniach z pkt 3.3; pojemność obejmuje przestrzeń na zapisy pakietów (F.05). Zamawiający nie ogranicza rodzaju, liczby, pojemności ani rozmieszczenia nośników pomiędzy komponentami. Dla komponentów wirtualnych wymaganie spełnia przydział dysków wirtualnych zgodnie z ofertą (A.06); nadmiarowość i wymienność nośników zapewnia wówczas platforma Zamawiającego.
T.06	**Lokalność danych operacyjnych.** Dane operacyjne Systemu (metadane, profile behawioralne i modele, artefakty wraz z sumami kontrolnymi, dane do analizy powłamaniowej) przechowywane są na lokalnej przestrzeni dyskowej dostarczonych komponentów, a nie na zasobach zewnętrznych (NAS, SAN, NFS, SMB, S3). Dla komponentów wirtualnych przestrzenią lokalną są przydzielone im dyski wirtualne, niezależnie od technologii przechowywania stosowanej przez platformę. Ograniczenie nie dotyczy archiwizacji (T.08) ani kopii zapasowych (F.46).

Nr	Wymaganie
T.07	**Retencja.** Retencja na lokalnej przestrzeni dyskowej: pełne, przeszukiwalne metadane sieciowe – co najmniej 45 dni; zdarzenia bezpieczeństwa wraz z kontekstem (hosty i usługi objęte zdarzeniem, klasyfikacja, powiązane IoC i artefakty), dostępne bezpośrednio w konsoli – co najmniej 365 dni; dziennik audytowy Systemu – co najmniej 12 miesięcy. Pełne metadane oznaczają rekord każdej sesji lub przepływu, bez próbkowania i bez agregacji w okresie retencji. Wymagane okresy retencji dotyczą ruchu nieprzekraczającego założeń z pkt 3.3 lit. a–d. Jeżeli przy takim ruchu retencja nie jest dotrzymana, Wykonawca w ramach wynagrodzenia rozbuduje pojemność w terminie 30 dni od stwierdzenia niedotrzymania. Zasady weryfikacji określa pkt 9.6.
T.08	**Archiwizacja.** Archiwizacja metadanych i zdarzeń na zasób zewnętrzny (SMB, NFS, SFTP, S3 lub równoważny) według harmonogramu, z możliwością odtworzenia lub przeszukania danych; archiwizacja nie jest warunkiem pracy Systemu i nie zastępuje retencji z T.07.

5.4. Obudowa, interfejsy, zasilanie i praca nadmiarowa

Nr	Wymaganie
T.09	**Obudowa i zasilanie.** Łączna wysokość dostarczanych komponentów fizycznych nie większa niż 4U, przy czym pojedynczy komponent nie wyższy niż 2U; montaż w szafie 19". Łączny maksymalny pobór mocy komponentów fizycznych, według kart katalogowych producenta (maximum power consumption), nie większy niż 1500 W; przy zasilaczach nadmiarowych nie sumuje się mocy znamionowej zasilaczy. Każdy komponent fizyczny wyposażony jest w nadmiarowe zasilacze wymieniane podczas pracy (hot-swap), umożliwiające zasilanie z dwóch niezależnych obwodów. Przewody zasilające zakończone wtykami C14 (IEC 60320).
T.10	**Interfejsy monitorujące.** Rozwiązanie zapewnia łącznie co najmniej 4 interfejsy monitorujące obsługujące wkładki 10GbE SFP+, umożliwiające jednoczesne podłączenie czterech łączy monitorujących (pkt 3.2); dopuszcza się rozłożenie interfejsów pomiędzy więcej niż jedną sondę oraz interfejsy o wyższej przepustowości (np. SFP28) obsługujące wkładki 10GbE bezpośrednio albo przez kable breakout. Interfejsy monitorujące pracują w trybie nasłuchu (receive-only) i są odrębne od interfejsów z T.11. Wykonawca dostarcza dla każdego z czterech łączy komplet umożliwiający jego zestawienie zgodnie z pkt 3.2: wkładki 10GbE SFP+ po stronie przełącznika (kompatybilne z platformą przełącznika wskazaną w pkt 3.2) i po stronie sondy (kompatybilne z kartą sondy) wraz z patchcordem o typie włókna, złączach i długości odpowiednich do medium i odległości z pkt 3.2, albo kabel DAC o długości odpowiedniej do odległości z pkt 3.2, poprawnie obsługiwany po obu stronach łącza. W przypadku sondy wirtualnej interfejsy monitorujące mogą być realizowane przez porty fizyczne hostów platformy Zamawiającego, przekazane do maszyny wirtualnej przez SR-IOV lub przez dedykowany przełącznik wirtualny, z zachowaniem odrębności od interfejsów zarządzających oraz wymagań T.01 i F.06. Wykonawca wskazuje w ofercie (Punkt 3.3 formularza ofertowego tj. Komponenty w formie c) – zasoby i porty (A.06, T.10 OPZ) – jeżeli dotyczy) liczbę i rodzaj wymaganych portów, wymagania dotyczące kart sieciowych oraz sposób przekazania portów do maszyny wirtualnej (A.06). Zapewnienie portów zgodnie z ofertą, w granicach limitu z pkt 3.1, leży po stronie Zamawiającego i nie stanowi rozbudowy sprzętowej hostów w rozumieniu A.06.

Nr	Wymaganie
T.11	**Interfejsy zarządzające.** Poza interfejsami monitorującymi każda sonda posiada co najmniej 1 interfejs zarządzający (out-of-band), odrębny od interfejsów monitorujących. Jeżeli mechanizm wysokiej dostępności oferowanego rozwiązania wymaga dedykowanego interfejsu (heartbeat, synchronizacja stanu), sonda posiada także taki interfejs. Zamawiający nie narzuca rodzaju złącza (RJ45 lub optyczne). Dla komponentów wirtualnych interfejsy te realizowane są jako odrębne interfejsy wirtualne, a funkcję portu konsoli pełni konsola maszyny wirtualnej.
T.12	**Praca nadmiarowa.** Architektura umożliwia dodanie w przyszłości komponentu przejmującego analizę ruchu z tych samych łączy monitorujących w razie awarii komponentu podstawowego, bez wymiany dostarczonego sprzętu i bez zmniejszania liczby interfejsów z T.10 i T.11. Zamawiający nie wymaga dostarczenia drugiego węzła; jego dodanie w przyszłości nie może wymagać zakupu licencji innej niż licencja drugiego węzła. Dla komponentu wirtualnego drugim węzłem może być druga instancja maszyny wirtualnej.

6. Wymagania funkcjonalne

6.1. Analiza ruchu i widoczność sieci

Nr	Wymaganie
F.01	**Analiza pasywna.** Pasywna analiza ruchu z portów lustrzanych (SPAN), agregatorów lub urządzeń TAP, w relacji północ–południe i wschód–zachód, bez wpływu na dostępność i wydajność sieci; System nie może wymagać pracy w trybie in-line.
F.02	**Protokoły i metadane.** Rozpoznawanie i dekodowanie protokołów warstwy aplikacji, co najmniej: HTTP, TLS/SSL, DNS, SMB/CIFS, LDAP, Kerberos, RDP, SSH, FTP, SMTP, DHCP, NTP, oraz gromadzenie przeszukiwalnych metadanych sesji: adresy i porty źródłowe i docelowe, protokół, znaczniki czasu, wolumen danych, a o ile możliwe do ustalenia – nazwa hosta, użytkownika i usługi.
F.03	**Inwentaryzacja urządzeń.** Automatyczna inwentaryzacja urządzeń widocznych w ruchu wraz z klasyfikacją: adres IP, a o ile adres MAC jest widoczny w ruchu – także adres MAC i producent na podstawie OUI; typ lub rola; aktywność w czasie – w postaci przeszukiwalnego i filtrowanego widoku.
F.04	**Ruch szyfrowany.** Zachowanie zdolności detekcyjnych dla ruchu szyfrowanego bez jego deszyfracji – w oparciu o metadane, parametry negocjacji sesji, charakterystyki statystyczne i wzorce zachowań – w tym analiza odcisków sesji TLS z wykorzystaniem cech strony klienta i serwera (JA3/JA3S, JA4/JA4S lub równoważny mechanizm).
F.05	**Pełne pakiety.** Rejestracja pełnych pakietów dla wybranych zdarzeń oraz wskazanych hostów i segmentów z możliwością pobrania pliku PCAP.
F.06	**Jakość widoczności.** Wykrywanie utraty pakietów na interfejsach monitorujących z alarmowaniem o przekroczeniu progu utraty widoczności. Rozpoznawanie i eliminowanie duplikatów pakietów i sesji otrzymanych w obrębie sondy z różnych łączy monitorujących lub z wielu sieci VLAN – w obrębie sondy statystyki, alarmy i metadane nie zliczają tego samego ruchu wielokrotnie. Sesja widoczna w więcej niż jednej sondzie daje w konsoli jeden alarm; jej metadane mogą być przechowywane w kopii z każdej sondy, z oznaczeniem sondy źródłowej.

Nr	Wymaganie
F.07	**Analiza powłamaniowa.** Widok analizy powłamaniowej (forensic) dla wykrytego zdarzenia, prezentujący w jednym miejscu chronologię powiązanych zdarzeń, hosty i usługi, zgromadzone metadane i artefakty oraz – dla zdarzeń o wysokim priorytecie – selektywnie zachowane dane ruchu; dane dostępne lokalnie, bez zależności od systemów zewnętrznych.

6.2. Detekcja behawioralna i profilowanie ruchu

Nr	Wymaganie
F.08	**Detekcja behawioralna.** Wykrywanie zagrożeń w oparciu o analizę behawioralną: automatyczne budowanie profilu (baseline) normalnej komunikacji i jego ciągła aktualizacja, bez ręcznego definiowania wzorca, z identyfikacją anomalii jako odchyleń od profilu i prezentacją przesłanek zgodnie z F.10; profile tworzone w zależności od adresu hosta oraz podsieci lub zdefiniowanej grupy adresów. Analiza behawioralna wykorzystuje uczenie maszynowe (ML) lub sztuczną inteligencję (AI), co Wykonawca potwierdza dokumentacją producenta, i jest uzupełniona detekcją sygnaturową i regułową.
F.09	**Grupy i segmenty.** Definiowanie własnych grup i segmentów (np. OT, centrum danych, stacje użytkowników, DMZ) oraz różnicowanie czułości detekcji, progów alarmowych i trybu reakcji odrębnie dla każdej grupy, w tym odrębne polityki dla segmentów OT i IT.
F.10	**Przesłanki detekcji.** Prezentacja przesłanek detekcji – wskazanie parametrów ruchu odbiegających od profilu wraz z wartościami obserwowanymi i miarą odchylenia od profilu (np. wartość oczekiwana, zakres typowy, percentyl).
F.11	**Zakres detekcji.** Wykrywanie co najmniej: komunikacji z serwerami sterującymi (C2), w tym beaconingu; algorytmów generowania domen (DGA) lub innych mechanizmów dynamicznego generowania nazw domenowych; ruchu bocznego; rekonesansu i skanowania sieci; eksfiltracji danych; tunelowania DNS; aktywności charakterystycznej dla ransomware; nadużycia kont i poświadczeń, w tym ataków siłowych; wykorzystania narzędzi zdalnego dostępu niezgodnych z polityką Zamawiającego.
F.12	**Reguły własne.** Samodzielne definiowanie przez administratora Zamawiającego własnych reguł detekcji i progów alarmowych.

6.3. Botnet, reputacja i wskaźniki kompromitacji

Nr	Wymaganie
F.13	**Botnet.** Wykrywanie aktywności botnet w oparciu o adresy IP oraz nazwy domenowe (analiza zapytań i odpowiedzi DNS), z prezentacją co najmniej nazwy botnetu lub rodziny zagrożenia, adresów IP i portów, hosta wewnętrznego oraz znacznika czasu, a o ile producent dysponuje taką informacją – także opisu działania zagrożenia i powiązanych technik MITRE ATT&CK.

Nr	Wymaganie
F.14	**Reputacja.** Identyfikowanie złośliwych adresów URL, domen i adresów IP w oparciu o bazę reputacyjną / threat intelligence producenta, aktualizowaną nie rzadziej niż raz na dobę, ze wskazaniem źródła wskaźnika, na podstawie którego wygenerowano detekcję. Zapytania zawierające dane Zamawiającego podlegają F.50.
F.15	**Własne i zewnętrzne IoC.** Zasilanie Systemu własnymi IoC Zamawiającego – wprowadzanymi ręcznie i importowanymi z pliku – oraz automatyczne pobieranie wskaźników ze źródeł zewnętrznych w standardzie STIX/TAXII lub równoważnym (np. MISP), w tym ze źródeł udostępnianych przez właściwy CSIRT, o ile są one udostępniane w standardzie STIX/TAXII lub w formacie MISP.

6.4. Ataki sieciowe i kryptografia

Nr	Wymaganie
F.16	**Ataki sieciowe.** Wykrywanie ataków sieciowych, w tym prób wykorzystania znanych podatności usług i aplikacji, ataków na protokoły oraz aktywności typu DoS w zakresie widocznym w analizowanym ruchu, z prezentacją co najmniej nazwy lub typu ataku, poziomu istotności, hosta źródłowego i docelowego, atakowanej usługi, opisu potencjalnego wpływu i rekomendowanego działania.
F.17	**Kryptografia i certyfikaty.** Wykrywanie słabych, przestarzałych lub wyłączonych mechanizmów kryptograficznych oraz komunikacji nieszyfrowanej podatnej na przechwycenie – co najmniej dla ośmiu protokołów spośród: TLS/SSL, SMB, HTTP, SIP, RTSP, SSH, POP3, IMAP, SMTP, SNMP, RDP, MySQL, PostgreSQL, Telnet, FTP, LDAP – oraz certyfikatów samopodpisanych, wygasłych, odwołanych lub niezgodnych z nazwą usługi.

6.5. Wykrywanie złośliwego oprogramowania

Nr	Wymaganie
F.18	**Wyodrębnianie plików.** Wyodrębnianie plików przenoszonych w ruchu sieciowym (SMB bez szyfrowania, HTTP, FTP, SMTP bez STARTTLS) i poddawanie ich analizie pod kątem złośliwej zawartości.
F.19	**Analiza złośliwego oprogramowania.** Wykrywanie i klasyfikowanie złośliwego oprogramowania bez uruchamiania pliku (analiza statyczna), realizowane na dostarczonych komponentach dowolnym mechanizmem (sygnaturowym, heurystycznym, statystycznym, reputacyjnym, ML lub ich kombinacją), silnikiem producenta Systemu albo silnikiem osadzonym w rozwiązaniu i objętym wsparciem producenta, z aktualizacją baz nie rzadziej niż raz na dobę. Dopuszcza się uzupełniającą weryfikację reputacji plików i sum kontrolnych w infrastrukturze producenta zlokalizowanej na terenie EOG oraz uzupełniającą analizę dynamiczną (sandbox) lokalnie lub w infrastrukturze producenta na terenie EOG; nie mogą one zastępować analizy statycznej, a ich niedostępność nie może ograniczać ani wstrzymywać detekcji.

Nr	Wymaganie
F.20	**Klasyfikacja i lista sum kontrolnych.** Klasyfikowanie wykrytego złośliwego oprogramowania według typów i rodzin, z prezentacją wyników w podziale na zainfekowane hosty, oraz prowadzenie listy sum kontrolnych plików traktowanych jako złośliwe (detekcja), z możliwością dodawania i usuwania wpisów przez administratora.
F.21	**Repozytorium artefaktów.** Przechowywanie próbek plików złośliwych wyodrębnionych z ruchu w repozytorium artefaktów, z możliwością przeglądu, pobrania i usunięcia z poziomu konsoli, oraz zestawienie zawierające nazwę pliku, sumę kontrolną, werdykt, hosty uczestniczące w transferze i znacznik czasu, w formacie maszynowo przetwarzalnym, dostępne w konsoli i przez REST API.

6.6. Środowisko przemysłowe OT/ICS/IoT

Nr	Wymaganie
F.22	**Protokoły przemysłowe.** Rozpoznawanie i parsowanie protokołów przemysłowych widocznych w punktach zbierania ruchu, wskazanych w pkt 3.1 (Segment OT), w zakresie, w jakim ruch nie jest szyfrowany; obsługa tych protokołów jest obligatoryjna.
F.23	**Urządzenia automatyki.** Rozpoznawanie urządzeń automatyki (PLC, HMI, RTU, stacje inżynierskie, przemienniki częstotliwości) komunikujących się przez punkty zbierania ruchu, wraz z identyfikacją producenta, a o ile możliwe do ustalenia z ruchu – modelu i wersji oprogramowania układowego.
F.24	**Operacje krytyczne.** Wykrywanie operacji krytycznych i potencjalnie nieautoryzowanych w protokołach objętych F.22: zmiany konfiguracji lub programu sterownika, przesłania lub pobrania programu, zmiany trybu pracy sterownika, dostępu inżynierskiego z hosta spoza listy dozwolonych.
F.25	**Tryb pasywny w OT.** Praca w segmencie OT wyłącznie w trybie pasywnym, bez aktywnego odpytywania urządzeń automatyki; funkcje aktywnego odpytywania, jeżeli występują, są domyślnie wyłączone, a zmiana tego ustawienia wymaga roli administratora i jest rejestrowana w dzienniku audytowym.
F.26	**Topologia OT.** Graficzna prezentacja topologii komunikacji w segmencie OT, z filtrowaniem po protokole i czasie.

6.7. Zdarzenia, wyszukiwanie, raportowanie i integracje

Nr	Wymaganie
F.27	**Karta zdarzenia i MITRE.** Karta zdarzenia zawierająca co najmniej: opis zagrożenia, poziom istotności, hosty uczestniczące w komunikacji, znaczniki czasu, zgromadzone dowody (metadane, artefakty, sumy kontrolne) oraz rekomendowane działanie; mapowanie zdarzeń na techniki MITRE ATT&CK z widokiem technik powiązanych z wykrytymi scenariuszami ataków, z opisem i odnośnikiem do szczegółów MITRE.

Nr	Wymaganie
F.28	**Wyszukiwanie zagrożeń i eksport.** Wyszukiwanie zagrożeń (threat hunting) w zgromadzonych metadanych i zdarzeniach w pełnym zakresie retencji z T.07, z filtrowaniem co najmniej po adresie IP, domenie lub URL, sumie kontrolnej pliku, porcie, protokole, nazwie hosta, poziomie istotności i przedziale czasu, oraz eksport wyników wyszukiwania i listy zdarzeń do co najmniej dwóch formatów spośród PDF, CSV, JSON, XLSX, w tym co najmniej jednego maszynowo przetwarzalnego.
F.29	**Pulpity i raporty.** Pulpity prezentujące stan bezpieczeństwa i obciążenia Systemu, z możliwością zdefiniowania własnego układu, oraz raporty generowane na żądanie i według ustalonego harmonogramu.
F.30	**SIEM i powiadomienia.** Przekazywanie zdarzeń jednocześnie do co najmniej dwóch odbiorców— protokołem syslog (RFC 5424), z treścią w co najmniej jednym z formatów CEF, LEEF, JSON i z polami określonymi w F.42; powiadamianie o zdarzeniach pocztą elektroniczną oraz przez syslog, z konfigurowalnymi progami istotności i listami adresatów. Wysyłka poczty przez przekaźnik poczty Zamawiającego (pkt 3.1), z obsługą TLS (STARTTLS), bez wymogu uwierzytelniania SMTP AUTH.
F.31	**REST API.** Udokumentowany interfejs REST API umożliwiający pobieranie zdarzeń, metadanych i wyników wyszukiwania oraz uruchamianie wyszukiwania retrospektywnego i pobieranie jego wyników (T.03, T.04).

6.8. Strojenie i ograniczanie liczby fałszywych alarmów

Nr	Wymaganie
F.32	**Strojenie.** Wyciszanie wybranych typów alarmów oraz alarmów dotyczących wskazanych hostów, podsieci, par komunikacyjnych lub okien czasowych, z wyodrębnionym widokiem wyciszonych alarmów i reguł (z informacją o użytkowniku i dacie wyciszenia) umożliwiającym ich ponowne włączenie. Wszystkie operacje strojenia, w tym zarządzanie listami wykluczeń (F.36), administrator Zamawiającego wykonuje samodzielnie z poziomu konsoli, bez udziału producenta lub Wykonawcy i bez dodatkowych kosztów; każda operacja jest rejestrowana w dzienniku audytowym.

6.9. Reakcja na zagrożenia — integracja z zaporą NGFW

Zasadniczym celem funkcjonalnym zamówienia jest aktywna reakcja na zagrożenie (System samodzielnie wymusza blokadę, bez udziału operatora) w czasie określonym w F.34), realizowana na posiadanej zaporze jako funkcja standardowa, udokumentowana i objęta wsparciem producenta (F.38, F.41). Reakcja obejmuje ruch przechodzący przez posiadaną zaporę: komunikację z Internetem oraz między segmentami routowanymi przez zaporę, wskazanymi w pkt 3.1. Zamawiający nie narzuca mechanizmu technicznego ani producenta systemu NDR.

Nr	Wymaganie
F.33	**Akcja blokująca.** Zainicjowanie akcji blokującej (blokada adresu IP, zakresu adresów lub hosta; dla adresów IPv4, a jeżeli według pkt 3.1 w sieci występuje IPv6 – także IPv6) na posiadanej zaporze jako następstwo detekcji, automatycznie albo poleceniem operatora w konsoli NDR, bez logowania administratora do interfejsu zarządzania zaporą i bez ręcznego przenoszenia danych między systemami. Tryb automatyczny pracuje w sposób ciągły, niezależnie od pory doby i bez wymogu aktywnej sesji operatora; o każdej wykonanej blokadzie System powiadamia pocztą elektroniczną oraz przez syslog do SIEM.
F.34	**Czas reakcji.** Czas od utworzenia alarmu spełniającego warunki reguły automatycznej reakcji (albo od zatwierdzenia akcji przez operatora) do momentu, w którym nowe połączenia objęte blokadą przestają być przepuszczane przez zaporę, nie przekracza 120 sekund – mierzony podczas testów (Załącznik nr 1, B3) na zaporze Zamawiającego jako mediana z co najmniej pięciu powtórzeń, przy czym żaden pojedynczy pomiar nie może przekroczyć 180 sekund. Pomiar: od czasu utworzenia alarmu w Systemie (nie czasu obserwowanej aktywności) do pierwszego odrzucenia połączenia testowego, nawiązywanego co 1 s z hosta testowego, zarejestrowanego w logu zapory przy włączonym logowaniu na regule blokującej; zegary obu systemów synchronizowane z tym samym serwerem NTP. Wymaganie dotyczy nowych połączeń; zerwanie sesji nawiązanych przed blokadą nie jest wymagane.
F.35	**Tryby reakcji.** Odrębne tryby reakcji – automatyczny i z zatwierdzeniem przez operatora – dla różnych segmentów sieci oraz typów i poziomów istotności zdarzeń, konfigurowane na poziomie polityki samodzielnie przez administratora Zamawiającego.
F.36	**Listy wykluczeń.** Definiowanie dwóch list wykluczeń: a) adresów i usług, których wskaźniki nie mogą zostać przekazane do zapory w żadnym trybie reakcji; b) adresów i usług wyłączonych z reakcji automatycznej, dla których dopuszczalna jest reakcja zatwierdzona przez operatora. Wykonawca konfiguruje listy na podstawie wykazu przekazanego przez Zamawiającego (pkt 7.3). Zdarzenie detekcyjne jest odnotowywane niezależnie od list.
F.37	**Cykl życia blokady.** Automatyczne wygaszanie wpisu blokującego po konfigurowalnym czasie oraz ręczne cofnięcie akcji z poziomu konsoli NDR. Prezentacja w konsoli statusu każdej akcji ze znacznikiem czasu, lista aktywnych blokad oraz rejestracja wszystkich akcji w dzienniku audytowym (znacznik czasu, operator lub reguła, zdarzenie źródłowe, przekazany wskaźnik, mechanizm, wynik operacji, moment wycofania). Statusy zależą od mechanizmu (F.38): a) mechanizmy, w których System wywołuje interfejs zapory – co najmniej: zlecona, wykonana, błąd, cofnięta, wygasła; statusy „wykonana" i „cofnięta" wynikają z odpowiedzi zapory na wywołanie albo z odczytu stanu wpisu na zaporze; b) mechanizmy, w których zapora pobiera wskaźniki z Systemu – co najmniej: opublikowana, wycofana z publikacji, wygasła, wraz z potwierdzeniem pobrania aktualnej listy przez zaporę, uzyskanym z rejestru pobrań kanału po stronie Systemu albo z odczytu stanu kanału na zaporze przez jej API.

Nr	Wymaganie
F.38	**Zgodność integracyjna i mechanizm.** Potwierdzona zgodność integracyjna z zaporą Zamawiającego, wykazana co najmniej jedną z okoliczności: a) rozwiązanie znajduje się na publicznie dostępnej liście rozwiązań zintegrowanych producenta zapory (Fabric-Ready / Technology Alliance lub równoważny wykaz); b) producent rozwiązania publikuje dokumentację integracji z FortiOS; c) producent rozwiązania publikuje i obejmuje wsparciem dokumentację eksportu wskaźników w formacie wykorzystywanym przez mechanizm zapory; d) rozwiązanie pochodzi od producenta zapory. Wykonawca wskazuje w ofercie adres publikacji. Mechanizm techniczny jest dowolny, w szczególności: konektor producenta, uwierzytelnione wywołanie REST API zapory, kanał wskaźników (threat feed / external connector) w trybie push albo pull z odświeżaniem co 1 minutę, STIX/TAXII, webhook, automatyzacja zapory (automation stitch) lub automatyzacja w posiadanym FortiAnalyzerze – o ile spełnione są pozostałe wymagania pkt 6.9. Komponenty, licencje lub subskrypcje wymagane po stronie zapory, których Zamawiający nie posiada (pkt 3.1), Wykonawca dostarcza w cenie oferty wraz ze wsparciem na ~~-~~Okres wsparcia.
F.39	**Bezpieczeństwo połączenia.** Połączenia między Systemem a zaporą są uwierzytelnione (token lub certyfikat)~~,~~ i szyfrowane. Jeżeli zastosowany mechanizm wymaga konta na zaporze, jest to dedykowane konto serwisowe (typu REST API Admin z tokenem), z profilem uprawnień ograniczonym do minimum niezbędnego dla tego mechanizmu, wykazanego w dokumentacji D.03, i z ograniczeniem dostępu do adresu Systemu (trusted hosts); obsługiwane są konteksty administracyjne (VDOM), jeżeli występują według pkt 3.1. Jeżeli zapora pobiera wskaźniki z Systemu, kanał wskaźników jest udostępniany wyłącznie przez HTTPS, z uwierzytelnieniem i ograniczeniem dostępu do adresów zapory.
F.40	**Odporność integracji.** Poprawne działanie integracji z zaporą pracującą w klastrze HA, w tym zachowanie ciągłości integracji i aktywnych blokad po przełączeniu węzłów, bez ponownej konfiguracji~~.~~. Poprawna obsługa niedostępności zapory: dla mechanizmów z F.37 lit. a – kolejkowanie lub ponawianie akcji~~,~~ i powiadomienie operatora; dla mechanizmów z F.37 lit. b – powiadomienie operatora, gdy zapora nie pobrała aktualnej listy w czasie dłuższym niż dwukrotność skonfigurowanego interwału odświeżania; w obu przypadkach bez utraty zdarzenia detekcyjnego i informacji o niewykonanej akcji.

Nr	Wymaganie
F.41	**Utrzymanie integracji.** Funkcjonalność F.33–F.40 dostępna w ramach ceny oferty, opisana w dokumentacji (D.03) i utrzymywana w sprawności przez cały Okres wsparcia, także po aktualizacjach oprogramowania NDR i zapory, z udokumentowanymi ograniczeniami ilościowymi mechanizmu wykorzystywanego po stronie zapory (maksymalna liczba i rozmiar wpisów, liczba kanałów, częstotliwość odświeżania). Mechanizm integracji jest funkcją opisaną w publicznej dokumentacji producenta systemu NDR lub producenta zapory i objętą wsparciem producenta; nie dopuszcza się integracji opartej na kodzie lub skryptach tworzonych przez Wykonawcę. Za kod lub skrypt tworzony przez Wykonawcę nie uznaje się konfiguracji mechanizmów opisanych w dokumentacji producenta systemu NDR lub zapory, w tym reguł automatyzacji z akcjami wbudowanymi; za taki kod uznaje się akcje typu „skrypt CLI" i inne skrypty, których treść przygotowuje Wykonawca. Obowiązek utrzymania dotyczy wersji FortiOS objętych wsparciem producenta zapory. Po wydaniu nowej gałęzi FortiOS Wykonawca przywraca pełną funkcjonalność integracji w terminie 30 dni od jej obsługi przez producenta systemu NDR, nie później niż 90 dni od zgłoszenia. Zamawiający informuje Wykonawcę o planowanej zmianie gałęzi FortiOS z wyprzedzeniem co najmniej 10 dni roboczych, a o aktualizacjach w obrębie gałęzi – nie później niż w dniu ich wykonania.
F.42	**Pola korelacyjne zdarzeń.** Zdarzenia detekcyjne i zdarzenia akcji blokujących przekazywane do SIEM (F.30) zawierają co najmniej: unikalny identyfikator zdarzenia, czas utworzenia alarmu i czas obserwowanej aktywności, adresy IP i porty źródłowe i docelowe, nazwę hosta i użytkownika (o ile zostały ustalone), protokół, kategorię i poziom istotności, technikę MITRE ATT&CK (o ile została przypisana), a dla akcji blokujących – przekazany wskaźnik, mechanizm i status akcji (F.37), co umożliwia ich korelację w SIEM z logami zapory. Odbieranie logów zapory przez System nie jest wymagane.

6.10. Zarządzanie, kontrola dostępu i utrzymanie

Nr	Wymaganie
F.43	**Konsola.** Konsola zarządzająca dostępna przez przeglądarkę (HTTPS, TLS 1.2 lub nowszy, z możliwością instalacji certyfikatu Zamawiającego), bez instalowania dedykowanego oprogramowania klienckiego, w języku polskim lub angielskim.
F.44	**Uwierzytelnianie i usługa katalogowa.** Integracja z Active Directory wyłącznie przez LDAPS lub LDAP z StartTLS, z weryfikacją certyfikatu kontrolera domeny, przy użyciu konta z uprawnieniami wyłącznie do odczytu katalogu, bez członkostwa w grupach uprzywilejowanych. Przypisanie użytkowników do adresów IP realizowane pasywnie z analizy ruchu uwierzytelniającego lub z dzienników przekazywanych przez SIEM; nie dopuszcza się wymagania uprawnień administracyjnych w domenie ani instalacji agentów na kontrolerach domeny. MFA dla kont administracyjnych: natywne (TOTP) albo przez Microsoft Entra ID (SAML 2.0 lub OpenID Connect).

Nr	Wymaganie
F.45	**Role i dziennik audytowy.** Kontrola dostępu oparta o role (RBAC) – co najmniej trzy rozłączne poziomy uprawnień (administrator, analityk, audytor), z możliwością definiowania ról własnych lub modyfikacji predefiniowanych – oraz dziennik audytowy działań użytkowników, zabezpieczony przed modyfikacją i usunięciem przez użytkownika bez uprawnień administracyjnych, z eksportem do SIEM.
F.46	**Kopia zapasowa.** Kopia zapasowa konfiguracji i bazy danych – ręcznie oraz według harmonogramu – z zapisem na zasób zewnętrzny (SMB, NFS, SFTP, S3 lub równoważny) oraz udokumentowana procedura odtworzenia.
F.47	**Monitorowanie stanu.** Monitorowanie stanu technicznego (procesor, pamięć, przestrzeń dyskowa, mechanizm wysokiej dostępności – jeżeli występuje, łączność, a dla komponentów fizycznych także stan macierzy, nośników i zasilaczy) z alarmowaniem o stanach awaryjnych, w tym o prognozowanym wyczerpaniu przestrzeni dyskowej zagrażającym retencji z T.07.
F.48	**Aktualizacje i czas.** Aktualizacja oprogramowania, sygnatur i modeli analitycznych możliwa w trybie bez dostępu do Internetu (air-gap), przez import pliku aktualizacyjnego; synchronizacja czasu z serwerem NTP wskazanym przez Zamawiającego oraz obsługa strefy czasowej Europe/Warsaw.

6.11. Bezpieczeństwo danych i suwerenność

Nr	Wymaganie
F.49	**Praca bez chmury.** Pełna funkcjonalność detekcyjna i zdolność do reakcji bez stałej łączności z chmurą producenta, w tym w trybie odseparowanym od Internetu, z aktualizacją z pliku (F.48); dopuszczalne jest okresowe pobieranie aktualizacji sygnatur, modeli i baz reputacyjnych.
F.50	**Lokalizacja danych.** Dane o ruchu sieciowym Zamawiającego – metadane, pakiety, pliki i ich sumy kontrolne – nie mogą być przetwarzane ani przechowywane poza terytorium Europejskiego Obszaru Gospodarczego. Wymóg obejmuje usługi reputacyjne (zapytania zawierające dane Zamawiającego), analizę dynamiczną i obsługę zgłoszeń. Przekazanie danych diagnostycznych poza EOG jest dopuszczalne wyłącznie za uprzednią zgodą Zamawiającego udzieloną dla danego zgłoszenia, po usunięciu zbędnych danych. Wykonawca wskazuje w ofercie (pkt 3.5 formularza ofertowego) lokalizacje przetwarzania danych dla każdej z tych usług. W zakresie, w jakim realizacja zamówienia wymaga dostępu do danych osobowych, Strony zawierają umowę powierzenia przetwarzania danych osobowych według wzoru stanowiącego część Dokumentów zamówienia.
F.51	**Producent.** Oferowane rozwiązanie nie obejmuje produktu ICT, usługi ICT ani procesu ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, ani produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 tej ustawy, lub usługi ICT albo procesu ICT określonych w takiej decyzji.
F.52	**Bezpieczeństwo Systemu.** Interfejsy zarządzania dostępne wyłącznie z sieci wskazanych przez Zamawiającego (lista dozwolonych adresów); możliwość wyłączenia nieużywanych usług; dostęp CLI wyłącznie przez SSHv2; brak aktywnych kont z hasłami fabrycznymi; monitorowanie stanu przez SNMPv3 (authPriv) i syslog.

7. Zakres prac

7.1. Wdrożenie

W ramach Wdrożenia Wykonawca:

- dostarczy System wraz z licencjami i subskrypcjami, kompletami do zestawienia łączy monitorujących (T.10) oraz wsparciem producenta;
- przeprowadzi analizę przedwdrożeniową i przekaże do akceptacji projekt techniczny obejmujący: punkty podłączenia i sposób pobierania ruchu, wynik weryfikacji sesji lustrzanych (źródła, kierunki, porty docelowe, ocena obciążenia), adresację, zakres integracji, harmonogram Wdrożenia i Optymalizacji, plan wycofania zmian oraz uszczegółowienie Programu testów (pkt 9.1);
- zamontuje komponenty fizyczne w szafie 19″ lub wdroży komponenty wirtualne na platformie Zamawiającego (import obrazu, przydział zasobów zgodnie z ofertą, konfiguracja sieci wirtualnych i przekazania ruchu) i podłączy łącza monitorujące;
- skonfiguruje moduły Systemu – silniki analityczne, detekcję zagrożeń i anomalii, mechanizmy wyszukiwania retrospektywnego (pkt 5.2), role użytkowników – oraz uruchomi funkcje wymagające okresu nauki w trybie nauki (F.08);
- zrealizuje integracje: z usługą katalogową (F.44); z przekaźnikiem poczty (F.30); z systemem zbierania logów – w zakresie konfiguracji wysyłki zdarzeń oraz wejścia i reguł parsowania;
- zestawi połączenie z zaporą z kontem serwisowym zgodnym z F.39 i wykona blokadę testową w trybie zatwierdzenia przez operatora (F.33, F.37);
- przeprowadzi test akceptacyjny (część A Programu testów), szkolenie podstawowe (S.01) i przekaże dokumentację powykonawczą (rozdział 11).

7.2. Optymalizacja

W ramach Optymalizacji Wykonawca:

- prowadzi naukę profilu (F.08), rozpoczętą z chwilą uruchomienia Systemu na ruchu produkcyjnym, a po jej zakończeniu – strojenie trwające nie krócej niż 14 dni, obejmujące przegląd wszystkich alarmów wygenerowanych w okresie strojenia i wykonanie działania strojącego (wyjątek, wyciszenie, korekta progu, reguły lub profilu) dla każdego alarmu zakwalifikowanego jako fałszywy (pkt 2.3); o kwalifikacji alarmu rozstrzyga zgodność jego przesłanek (F.10) z rzeczywistym stanem ruchu, ustalona na podstawie metadanych i zapisów pakietów;
- konfiguruje zasady automatycznej reakcji (F.33–F.37), w tym tryby reakcji dla segmentów i typów zdarzeń (F.35) oraz listy wykluczeń na podstawie wykazu przekazanego przez Zamawiającego (F.36);
- przeprowadza testy części B Programu testów, w tym pomiar czasu blokady (F.34), test 72-godzinny i test obciążeniowy (T.01) oraz weryfikację retencji i czasu wyszukiwania (pkt 9.6);
- przeprowadza szkolenie rozszerzone (S.01) i przekazuje dokumentację końcową wraz z raportem ze strojenia (rozdział 11).

Po podpisaniu protokołu zakończenia Optymalizacji Wykonawca w ramach wsparcia (priorytet standardowy) przekazuje rekomendację działania strojącego dla zgłoszonych fałszywych alarmów, a gdy przyczyną fałszywego alarmu jest wada oprogramowania – usuwa ją.

7.3. Warunki prowadzenia prac i obowiązki Zamawiającego

- Prace ingerujące w konfigurację sieci produkcyjnej, zapory lub platformy wirtualizacyjnej realizowane są wyłącznie w oknach serwisowych, w obecności przedstawiciela Zamawiającego, z planem wycofania zmian (rollback) dla każdego etapu. Zamawiający udostępnia okno serwisowe w terminie 2 dni roboczych od wniosku Wykonawcy.
- Każda zmiana konfiguracji zapory wymaga uprzedniej akceptacji Zamawiającego i udokumentowania; Wykonawca nie wprowadza zmian w konfiguracji urządzeń automatyki przemysłowej.

Zamawiający:

a) zapewnia skonfigurowane sesje lustrzane (pkt 3.1) i wprowadza zmiany wynikające z ich weryfikacji w terminie 2 dni roboczych od zgłoszenia przez Wykonawcę;

b) udostępnia zasoby maszyn wirtualnych zgodne z ofertą w terminie 2 dni roboczych od wyboru oferty, a jeżeli oferta tego wymaga – przygotowuje hosty platformy wirtualizacyjnej do przekazania portów (IOMMU, SR-IOV) w terminie 3 dni roboczych od zawarcia umowy, w oknie serwisowym;

c) akceptuje projekt techniczny albo zgłasza do niego uwagi w terminie 2 dni roboczych od jego otrzymania;

d) przekazuje w analizie przedwdrożeniowej dane konfiguracyjne (pkt 3.1), wykaz do list wykluczeń (F.36) oraz listę kontrolną hostów i urządzeń do testu inwentaryzacji (Załącznik nr 1, A5);

e) zapewnia przekaźnik poczty dla adresu Systemu (pkt 3.1) oraz konto do odczytu katalogu (F.44);

f) zapewnia warunki testów określone w pkt 9.2.

Skutki niewykonania obowiązków Zamawiającego w terminie, w tym przesłanki zmiany terminów z rozdziału 8, określa wzór umowy.

8. Terminy

- Projekt techniczny – w terminie 5 dni roboczych od dnia zawarcia umowy; uwagi Zamawiającego Wykonawca uwzględnia w terminie 2 dni roboczych od ich otrzymania.
- Odbiór wdrożenia – do dnia 9.12.2026 r.
- Zakończenie Optymalizacji (podpisanie protokołu zakończenia Optymalizacji) – do dnia 31.03.2027 r.

Termin Odbioru wdrożenia wynika z okresu realizacji projektu finansowanego z grantu, który kończy się 31.12.2026 r. Skutki opóźnienia oraz przesłanki zmiany terminów określa wzór umowy.

9. Testy i odbiory

9.1. Zasady ogólne

Testy odbiorcze przeprowadza się stacjonarnie w środowisku produkcyjnym Zamawiającego, na rzeczywistym ruchu i posiadanych urządzeniach (w tym na zaporze), z udziałem inżyniera Wykonawcy odpowiedzialnego za wdrożenie oraz pracowników technicznych Zamawiającego, według Programu testów: część A (test akceptacyjny) warunkuje Odbiór wdrożenia, a część B – podpisanie protokołu zakończenia Optymalizacji. Przebieg testów dokumentuje się w Karcie Weryfikacji Funkcjonalnej, stanowiącej załącznik do odpowiedniego protokołu.

Program testów jest wiążący. W projekcie technicznym Strony uzgadniają jego uszczegółowienie (adresy, narzędzia, terminy), bez zmiany kryteriów zaliczenia; w razie braku uzgodnienia w terminie 5 dni roboczych od przekazania projektu technicznego stosuje się Program testów w brzmieniu Załącznika nr 1, a narzędzia testowe

wskazuje Wykonawca. Wymagania nieobjęte Programem testów weryfikuje się na podstawie konfiguracji i dokumentacji producenta.

Symulacje ataków wykonuje Wykonawca narzędziami wskazanymi w projekcie technicznym, wyłącznie z hosta testowego i wyłącznie poza segmentem OT. Testy wymagające ingerencji w działanie zapory przeprowadza się w oknie serwisowym z planem wycofania; niedostępność zapory symuluje się przez czasowe odebranie dostępu kontu integracyjnemu albo zablokowanie komunikacji Systemu z zaporą, a nie przez jej wyłączenie.

Powtórzenie testów obejmuje scenariusze zakończone wynikiem negatywnym oraz scenariusze, na które wpłynęły wprowadzone poprawki. Test przerwany z przyczyn leżących po stronie Zamawiającego kontynuuje się następnego dnia roboczego; czas przerwy nie jest wliczany do czasu trwania testu.

9.2. Obowiązki Zamawiającego w testach

Na czas testów Zamawiający:

a) zapewnia host testowy w segmencie IT wskazanym w projekcie technicznym, z uprawnieniami pozwalającymi na uruchomienie narzędzi testowych oraz udział testowy SMB bez szyfrowania i konto testowe na serwerze testowym (Załącznik nr 1, B2);

b) udziela pisemnej zgody na symulacje ataków, określającej ich zakres, czas, adresy i narzędzia;

c) uprzedza operatora SOC/MDR o terminie i zakresie symulacji;

d) wprowadza w systemie EDR wyjątki dla hosta testowego i narzędzi testowych;

e) zapewnia potwierdzenie odbioru zdarzeń testowych oraz akceptuje włączenie logowania na regule blokującej zapory (F.34).

9.3 Protokół dostawy

Po dostarczeniu komponentów Strony podpisują protokół dostawy potwierdzający zgodność z ofertą: numery seryjne, wersje oprogramowania, licencje i subskrypcje (nazwa, ilość, okres ważności, rejestracja na Zamawiającego) oraz komplety do zestawienia łączy (T.10). Dla komponentów wirtualnych protokół obejmuje wersje obrazów, przydzielone zasoby i licencje. Wraz z protokołem Wykonawca przekazuje potwierdzenie rejestracji numerów seryjnych, licencji i wsparcia na portalu producenta (A.04, A.08). Protokół dostawy nie stanowi podstawy do wystawienia faktury.

9.4. Odbiór wdrożenia

Odbiór wdrożenia następuje po łącznym spełnieniu warunków:

a) pozytywny wynik testu akceptacyjnego (wszystkie scenariusze części A Programu testów);

b) przeprowadzenie szkolenia podstawowego (S.01);

c) przekazanie dokumentacji powykonawczej (rozdział 11).

Wykonawca zgłasza gotowość do testu akceptacyjnego z wyprzedzeniem co najmniej 2 dni roboczych. Test akceptacyjny trwa nie dłużej niż 2 dni robocze.

Przy wyniku negatywnym Wykonawcy przysługuje jednokrotne powtórzenie testu w terminie 3 dni roboczych; powtórzenie nie zmienia terminu Odbioru wdrożenia określonego w rozdziale 8.

Usterki, które nie uniemożliwiają pozytywnego wyniku żadnego scenariusza–części A, nie wstrzymują Odbioru wdrożenia; wpisuje się je do protokołu wraz z terminem usunięcia 10 dni roboczych.

Protokół odbioru wdrożenia zawiera wykaz dostarczonego sprzętu, licencji i subskrypcji (nazwa, ilość, numery, okres ważności), datę uruchomienia Systemu na ruchu produkcyjnym oraz wyniki testu akceptacyjnego. Podpisany protokół stanowi podstawę do wystawienia faktury (pkt 1.3).

9.5. Zakończenie Optymalizacji

Protokół zakończenia Optymalizacji Strony podpisują po łącznym spełnieniu warunków:

a) pozytywny wynik scenariuszy B1–B5 części B Programu testów, w tym pomiaru czasu blokady (F.34), testu 72-godzinnego i testu obciążeniowego (T.01);

b) pozytywny wynik weryfikacji retencji i czasu wyszukiwania (scenariusz B6, pkt 9.6);

c) przekazanie raportu ze strojenia (D.05) wykazującego, że każdy alarm z okresu strojenia zakwalifikowany jako fałszywy został objęty działaniem strojącym;

d) przeprowadzenie szkolenia rozszerzonego (S.01);

e) przekazanie dokumentacji końcowej (rozdział 11).

Do testów części B stosuje się zasady zgłaszania gotowości, powtórzenia testu i usterek z pkt 9.4, przy czym powtórzenie nie zmienia terminu zakończenia Optymalizacji określonego w rozdziale 8; powtórzenie weryfikacji retencji odbywa się na zasadach pkt 9.6. Czas trwania poszczególnych testów określa Program testów. Protokół zakończenia Optymalizacji nie stanowi podstawy do odrębnego wynagrodzenia (pkt 1.3); skutki opóźnienia określa wzór umowy.

9.6. Weryfikacja retencji i czasu wyszukiwania

Retencję (T.07) i czas wyszukiwania w pełnym zakresie retencji (T.03) weryfikuje się jednokrotnie, w ramach części B Programu testów, w obecności Wykonawcy, po upływie co najmniej 45 dni pracy Systemu na ruchu produkcyjnym, liczonych od daty wskazanej w protokole odbioru wdrożenia:

a) metadane – wyszukiwanie zwraca pełne metadane z okresu co najmniej 45 dni wstecz;

b) zdarzenia (365 dni) i dziennik audytowy (12 miesięcy) – na podstawie przyrostu danych w okresie weryfikacji i dostępnej pojemności (prognoza z raportu D.05);

c) czas wyszukiwania – wyszukiwanie po sumie kontrolnej w pełnym zakresie retencji metadanych trwa nie dłużej niż 5 minut (T.03).

Jeżeli w okresie weryfikacji średni dobowy wolumen ruchu (według liczników portów docelowych sesji lustrzanych) lub średnia dobowa liczba nowych sesji (według rejestrów Systemu) przekroczyły założenia z pkt 3.3 lit. c–d, wymagany okres retencji metadanych wynosi 45 dni pomnożone przez mniejszy ze stosunków wartości z założeń do wartości zmierzonej. Niedotrzymanie retencji Wykonawca usuwa w trybie T.07, a weryfikację powtarza się po rozbudowie pojemności; spełnienie wymagania potwierdza wówczas przyrost danych w okresie weryfikacji i pojemność dostępna po rozbudowie. Pozytywny wynik weryfikacji jest warunkiem podpisania protokołu zakończenia Optymalizacji (pkt 9.5).

10. Szkolenia

Nr	Wymaganie
S.01	**Forma i wymiar.** Szkolenia stacjonarne w siedzibie Zamawiającego dla co najmniej 2 pracowników, w łącznym wymiarze co najmniej 16 godzin zegarowych: szkolenie podstawowe – co najmniej 8 godzin, przed Odbiorem wdrożenia; szkolenie rozszerzone – co najmniej 8 godzin, w Optymalizacji, po skonfigurowaniu zasad automatycznej reakcji. Szkolenia mają charakter praktyczny (warsztatowy) i są prowadzone na instalacji Zamawiającego; niedopuszczalne jest prowadzenie ich wyłącznie w formie prezentacji handlowej lub odtwarzania nagrań. Szkolenia prowadzone są w języku polskim albo z tłumaczeniem zapewnionym przez Wykonawcę.
S.02	**Prowadzący.** Szkolenia prowadzi inżynier posiadający aktualny certyfikat techniczny producenta oferowanego rozwiązania lub potwierdzenie ukończenia autoryzowanego szkolenia producenta, który uczestniczył we wdrożeniu i ma udokumentowane doświadczenie w co najmniej jednym wdrożeniu oferowanego rozwiązania; dopuszcza się prowadzenie szkoleń przez inżyniera producenta. Dokumenty potwierdzające kwalifikacje prowadzącego Wykonawca przekazuje co najmniej 2 dni robocze przed szkoleniem; warunek udziału we wdrożeniu nie dotyczy inżyniera producenta.
S.03	**Zakres i materiały.** Szkolenie podstawowe obejmuje co najmniej: architekturę wdrożenia, łącza monitorujące i diagnostykę widoczności; bieżącą administrację (kopie zapasowe, aktualizacje online i offline, monitorowanie stanu i zajętości dysku, archiwizacja); analizę zdarzeń (pulpity, MITRE ATT&CK, analiza powłamaniowa, wyszukiwanie zagrożeń, wyszukiwanie retrospektywne, repozytorium artefaktów); zgłaszanie problemów do wsparcia. Szkolenie rozszerzone obejmuje co najmniej: strojenie i zarządzanie wyjątkami; integracje i reakcję na zaporze (oba tryby, listy wykluczeń, wygaszanie, cofanie i przegląd blokad); diagnostykę typowych problemów; omówienie raportu ze strojenia. Materiały w języku polskim lub angielskim, w formie elektronicznej, z prawem do powielania na potrzeby wewnętrzne; imienne zaświadczenia dla uczestników.

11. Dokumentacja

Wykonawca dostarczy dokumentację w języku polskim, w wersji edytowalnej oraz PDF: dokumentację powykonawczą (D.01–D.04), której przekazanie jest warunkiem Odbioru wdrożenia, oraz dokumentację końcową (D.01–D.04 zaktualizowane o konfigurację po Optymalizacji oraz D.05), której przekazanie jest warunkiem podpisania protokołu zakończenia Optymalizacji. Dokumentacja produktowa producenta (podręczniki, noty techniczne) może być dostarczona w języku angielskim. Niedopuszczalne jest zastąpienie dokumentacji ogólnym spisem funkcji Systemu lub tłumaczeniem materiałów marketingowych.

Nr	Wymaganie
D.01	**Architektura i komponenty.** Fizyczny i logiczny schemat podłączenia, porty i wkładki, adresacja IP, sieci VLAN, zakres sesji lustrzanych, a dla komponentów wirtualnych – konfiguracja maszyn wirtualnych (zasoby, rezerwacje, typ procesora, dyski i sieci wirtualne, przekazanie ruchu); wykaz komponentów z numerami seryjnymi lub identyfikatorami instancji, wersjami oprogramowania i obrazów, numerami licencji, datami ważności wsparcia i kontaktami do wsparcia producenta.

Nr	Wymaganie
D.02	**Polityki i uprawnienia.** Konfiguracja polityk detekcji i reakcji – podział na segmenty, tryby reakcji, listy wykluczeń – wraz z uzasadnieniem przyjętych ustawień oraz macierz ról i uprawnień (RBAC) z opisem zakresu każdej roli.
D.03	**Integracje.** Opis zrealizowanych integracji: metody i punkty końcowe API, sposób uwierzytelniania, konta serwisowe i wykaz ich uprawnień, procedury testowe; dla integracji z zaporą dodatkowo mechanizm i statusy akcji (F.37), procedura cofnięcia blokady i przeglądu blokad aktywnych, zachowanie przy przełączeniu klastra HA, ograniczenia ilościowe mechanizmu (F.41), a w dokumentacji końcowej – zmierzony czas blokady (F.34).
D.04	**Procedury.** Procedury krok po kroku: kopia zapasowa i odtworzenie, odtworzenie Systemu po awarii sprzętowej lub awarii platformy wirtualizacyjnej (ponowne wdrożenie maszyny wirtualnej i przywrócenie danych); instrukcje stanowiskowe: obsługa incydentu, wyciszanie fałszywych alarmów i wyjątki, cofnięcie blokady wykonanej automatycznie, aktualizacja Systemu i baz sygnatur, zgłoszenie do wsparcia technicznego.
D.05	**Raport ze strojenia.** Daty rozpoczęcia i zakończenia nauki profilu oraz okresu strojenia; zestawienie alarmów z okresu strojenia wraz z ich kwalifikacją (fałszywy, prawdziwy, dotyczący ruchu dozwolonego) i podjętymi działaniami strojącymi, liczba alarmów przed strojeniem i po nim, wykaz wprowadzonych wyjątków i zmian konfiguracji oraz prognoza zajętości przestrzeni dyskowej potwierdzająca dotrzymanie retencji z T.07.

12. Wsparcie techniczne i poziomy usług (SLA)

Nr	Wymaganie
U.01	**Okres wsparcia.** Wsparcie techniczne Wykonawcy i producenta w Okresie wsparcia (pkt 2.3), obejmujące dostęp do aktualizacji oprogramowania, sygnatur, baz reputacyjnych i modeli analitycznych.
U.02	**Zgłoszenia i eskalacja.** Zgłoszenia przyjmowane telefonicznie, pocztą elektroniczną i przez portal zgłoszeniowy: 24/7/365 dla zgłoszeń krytycznych, w godzinach roboczych (pkt 2.3) dla pozostałych. Wsparcie pierwszej i drugiej linii w języku polskim; wsparcie producenta (trzecia linia) może być świadczone w języku angielskim, przy czym obsługę zgłoszenia i komunikację z Zamawiającym prowadzi Wykonawca w języku polskim. Wykonawca eskaluje do producenta problemy nierozwiązywalne na swoim poziomie i udostępnia Zamawiającemu dane kontaktowe wsparcia producenta.
U.03	**Wymiana sprzętu.** Wymiana uszkodzonego sprzętu dostarczonego w ramach zamówienia w trybie NBD lub lepszym przez cały Okres wsparcia. Przy awarii sprzętowej komponentu fizycznego czasem naprawy, niezależnie od priorytetu zgłoszenia, jest wymiana sprzętu w tym trybie; czas reakcji pozostaje zgodny z tabelą 12.1. Uszkodzone nośniki danych pozostają u Zamawiającego; Wykonawca nie żąda ich zwrotu, a związany z tym koszt jest objęty ceną oferty. Wymiana całego komponentu fizycznego następuje po wymontowaniu i przekazaniu Zamawiającemu jego nośników albo po ich zniszczeniu w obecności Zamawiającego, potwierdzonym protokołem.

Nr	Wymaganie
U.04	**Awaria platformy Zamawiającego.** Przy komponentach wirtualnych niedostępność lub nieprawidłowe działanie Systemu wynikające z awarii platformy wirtualizacyjnej Zamawiającego nie stanowi naruszenia czasów reakcji ani naprawy przez Wykonawcę. Niezapewnienie przez Zamawiającego zasobów lub parametrów wskazanych w ofercie (A.06), w tym wydajności przestrzeni dyskowej i ustawień procesora maszyny wirtualnej, obciąża Zamawiającego. Za awarię platformy nie uznaje się niedostępności wynikającej z niewystarczających zasobów, jeżeli Zamawiający przydzielił zasoby i parametry wskazane w ofercie ~~(A.06)~~; Wykonawca, który powołuje się na awarię platformy, wykazuje jej wpływ na działanie Systemu. Po przywróceniu sprawności platformy Wykonawca, w ramach wsparcia i bez dodatkowego wynagrodzenia, przywraca działanie komponentów wirtualnych (D.04); zgłoszenie obsługiwane jest z priorytetem wysokim, a czasy reakcji i naprawy liczone są od udostępnienia sprawnej platformy.
U.05	**Utrzymanie integracji z zaporą.** Utrzymanie w sprawności integracji z zaporą na zasadach F.41. Przywrócenie sprawności integracji obsługiwane jest jako zgłoszenie o priorytecie wysokim, z wyjątkiem dostosowania do nowej gałęzi FortiOS, do którego stosuje się terminy z F.41.
U.06	**Obsługa podatności.** Wykonawca informuje Zamawiającego o podatnościach dostarczonych komponentów w ciągu 2 dni roboczych od publikacji biuletynu producenta i wdraża poprawkę albo obejście: dla podatności ocenionych przez producenta jako krytyczne (CVSS 9,0 lub więcej według oceny podanej w biuletynie producenta) – w ciągu 7 dni, a dla ocenionych jako wysokie (CVSS 7,0–8,9) – w ciągu 30 dni, licząc od późniejszej z dat: udostępnienia poprawki przez producenta albo udostępnienia okna serwisowego przez Zamawiającego.
U.07	**Definicje SLA.** Czas reakcji – czas od zarejestrowania zgłoszenia do kontaktu inżyniera Wykonawcy podejmującego diagnozę. Czasy dla priorytetu krytycznego liczone są w godzinach zegarowych, dla pozostałych – w godzinach roboczych (pkt 2.3). Obejście przywraca funkcję i zatrzymuje bieg czasu naprawy; naprawa trwała następuje w terminie 30 dni od obejścia. Priorytet nadaje Zamawiający zgodnie z definicjami z tabeli 12.1. Tryb NBD określa pkt 2.3.

~~SLA~~ Tabela 12.1. Poziomy usług

Priorytet	Definicja	Czas reakcji	Czas obejścia ~~/~~lub naprawy
Krytyczny	Całkowity brak działania Systemu lub utrata funkcji detekcji	4 godz.	8 godz.; przy awarii sprzętowej komponentu fizycznego – NBD (U.03)
Wysoki	Istotne ograniczenie funkcjonalności, brak jednej z integracji, w tym integracji z zaporą	8 godz.	2 dni robocze
Standardowy	Pozostałe zgłoszenia, pytania konfiguracyjne	24 godz.	10 dni roboczych

Załącznik nr 1. Program testów odbiorczych

Program określa scenariusze testów, ich przebieg i kryteria zaliczenia. Część A stanowi test akceptacyjny warunkujący Odbiór wdrożenia (pkt 9.4), część B – testy warunkujące podpisanie protokołu zakończenia Optymalizacji (pkt 9.5). Adresy, narzędzia i terminy uszczegóławia projekt techniczny (pkt 9.1). Scenariusz jest zaliczony, gdy spełnione są wszystkie jego kryteria. Symulacje ataków wykonuje się wyłącznie z hosta testowego, poza segmentem OT, na warunkach pkt 9.2.

Część A. Test akceptacyjny (Wdrożenie)

Nr	Scenariusz i wymagania	Przebieg	Kryterium zaliczenia
A1	Widoczność łączy (F.01, F.06, T.10)	Przez 15 min Zamawiający odczytuje co 1 min liczniki pakietów portów docelowych sesji lustrzanych, a Wykonawca – liczniki pakietów odebranych i odrzuconych przez interfejsy monitorujące Systemu.	Ruch odbierany ze wszystkich czterech łączy; dla każdego łącza liczba pakietów odebranych przez System nie mniejsza niż 99 % wskazania licznika portu docelowego; brak odrzuceń pakietów z powodu braku zasobów.
A2	Deduplikacja (F.06)	Z hosta testowego nawiązanie sesji przechodzącej przez oba punkty zbierania, wywołującej alarm reguły testowej (F.12) lub wskaźnika testowego (F.15).	W konsoli jeden alarm dla sesji testowej; w obrębie każdej sondy jeden rekord sesji; metadane z więcej niż jednej sondy oznaczone sondą źródłową.
A3	Detekcja wskaźników i skanowania (F.11, F.13–F.15, F.27)	Dodanie testowych IoC (adres IP i domena); z hosta testowego: połączenia z adresem testowym, zapytania DNS o domenę testową oraz skanowanie portów w zakresie adresów IT wskazanym w projekcie technicznym.	Dla każdej symulacji alarm z kartą zdarzenia zawierającą elementy F.27 i wskazaniem źródła wskaźnika, wygenerowany w ciągu 15 min od rozpoczęcia symulacji.
A4	Pliki i zasięg incydentu (F.18–F.21, T.02, T.03)	Przesłanie z hosta testowego pliku testowego rozpoznawanego jako złośliwy (np. plik testowy EICAR albo próbka wskazana w projekcie technicznym) oraz pliku nieszkodliwego przez SMB bez szyfrowania (obowiązkowo) i co najmniej jeden z protokołów: HTTP, FTP, SMTP bez STARTTLS; następnie wyszukanie po SHA-256 każdego pliku.	Pliki wyodrębnione ze wszystkich użytych protokołów; sumy SHA-256, SHA-1 i MD5 powiązane z sesją, hostami, protokołem, kierunkiem i czasem; plik testowy złośliwy sklasyfikowany jako złośliwy i umieszczony w repozytorium artefaktów; wyszukiwanie zwraca wszystkie wystąpienia w zgromadzonych danych w czasie nie dłuższym niż 5 min.

Nr	Scenariusz i wymagania	Przebieg	Kryterium zaliczenia
A5	Inwentaryzacja i OT (F.03, F.22, F.23, F.25, F.26)	Przegląd inwentarza po co najmniej 24 h pracy na ruchu produkcyjnym wobec listy kontrolnej Zamawiającego (pkt 7.3 lit. d: co najmniej 20 hostów IT oraz urządzenia automatyki komunikujące się przez punkty zbierania); przegląd ustawień aktywnego odpytywania.	Hosty i urządzenia z listy kontrolnej aktywne w okresie testu widoczne w inwentarzu z adresem IP, a gdy adres MAC jest widoczny – także z adresem MAC i producentem; sesje protokołów przemysłowych z pkt 3.1 występujące w ruchu rozpoznane i sparsowane w zakresie ruchu nieszyfrowanego; topologia OT prezentowana; funkcje aktywnego odpytywania wyłączone.
A6	Integracje (F.30, F.42–F.44)	Przekazanie zdarzeń z A3 do systemu zbierani logów; logowanie do konsoli kontem z Active Directory i z MFA; powiadomienie e-mail o zdarzeniu testowym.	Zdarzenia zarejestrowane w systemie zbierania logów z polami F.42 rozdzielonymi przez reguły parsowania; logowanie przez LDAPS lub StartTLS z weryfikacją certyfikatu i z MFA; wiadomość dostarczona do skrzynki testowej przez przekaźnik poczty.
A7	Połączenie z zaporą (F.33, F.37, F.39)	Operator zleca z konsoli NDR blokadę adresu testowego, sprawdza ją w logu zapory, a następnie ją cofa.	Połączenia z adresem testowym odrzucane przez zaporę po blokadzie i przepuszczane po jej cofnięciu; statusy akcji zgodne z F.37 dla zastosowanego mechanizmu; akcje w dzienniku audytowym; uprawnienia konta serwisowego (jeżeli mechanizm go wymaga) zgodne z wykazem w D.03.
A8	Administracja i bezpieczeństwo (F.45–F.48, F.52)	Utworzenie kont w trzech rolach; kopia zapasowa na zasób zewnętrzny; aktualizacja sygnatur (online albo z pliku); próba dostępu do interfejsu zarządzania spoza dozwolonych sieci; odczyt stanu przez SNMPv3.	Role działają zgodnie z F.45; kopia zapisana na zasobie zewnętrznym; aktualizacja zakończona; dostęp spoza dozwolonych sieci odrzucony; odczyt SNMPv3 (authPriv) poprawny.

Część B. Testy Optymalizacji

Nr	Scenariusz i wymagania	Przebieg	Kryterium zaliczenia
B1	Strojenie (pkt 7.2, D.05)	Przegląd raportu ze strojenia wobec alarmów zarejestrowanych w Systemie w okresie strojenia.	Każdy alarm z okresu strojenia zakwalifikowany jako fałszywy objęty działaniem strojącym wykazanym w raporcie; okres strojenia nie krótszy niż 14 dni od zakończenia nauki profilu.
B2	Detekcja behawioralna (F.08, F.10, F.11)	Po zakończeniu nauki profilu, z hosta testowego: a) połączenia HTTPS z adresem testowym w Internecie w stałym odstępie 60 s przez 2 h; b) zapytania DNS z danymi zakodowanymi w nazwach do domeny testowej przez 30 min; c) co najmniej 50 nieudanych prób logowania do konta testowego na serwerze testowym (np. przez SMB, RDP albo SSH) w ciągu 5 min.	Dla każdej symulacji alarm z przesłankami zgodnymi z F.10, wygenerowany w czasie trwania symulacji lub w ciągu 60 min od jej zakończenia.
B3	Reakcja automatyczna i czas blokady (F.33–F.36)	Reguła automatycznej reakcji dla wskaźnika testowego; host testowy nawiązuje połączenie z adresem testowym co 1 s; pięć powtórzeń. Dodatkowo wskaźniki testowe z adresami z list wykluczeń a i b (F.36).	Mediana czasu blokady (F.34) nie dłuższa niż 120 s, żaden pomiar dłuższy niż 180 s; powiadomienie e-mail i syslog o każdej blokadzie; adres z listy a nieprzekazany do zapory, adres z listy b zablokowany dopiero po zatwierdzeniu przez operatora; zdarzenie detekcyjne odnotowane w każdym przypadku.
B4	Odporność integracji (F.40)	W oknie serwisowym: czasowe odebranie dostępu kontu integracyjnemu albo zablokowanie komunikacji Systemu z zaporą i zlecenie blokady, a następnie przywrócenie łączności. Przełączenie węzłów klastra HA zapory – jeżeli Zamawiający wyrazi na nie zgodę; w przeciwnym razie weryfikacja na podstawie dokumentacji (D.03).	Operator powiadomiony o niewykonanej akcji; zdarzenie detekcyjne zachowane; po przywróceniu łączności akcja wykonana z ponowienia albo oznaczona jako błąd; aktywne blokady zachowane po przełączeniu węzłów klastra.

Nr	Scenariusz i wymagania	Przebieg	Kryterium zaliczenia
B5	Test 72-godzinny (pkt 2.3, T.01, F.06)	72 h pracy na ruchu rzeczywistym, obejmujące trzy dobowe szczyty; odczyt liczników jak w A1, co 1 min; w trakcie testu co najmniej trzy wyszukiwania retrospektywne (T.03) i wygenerowanie raportu (F.29).	W każdym interwale 1 min z ruchem nieprzekraczającym 3 Gb/s spełniona definicja braku utraty pakietów (pkt 2.3).
B6	Retencja i czas wyszukiwania (T.03, T.07)	Weryfikacja według pkt 9.6.	Wynik pozytywny według pkt 9.6.