Opis przedmiotu zamówienia

na

dostawę, wdrożenie systemu do analizy, detekcji i prewencji zagrożeń w ruchu sieciowym oraz na stacjach końcowych i serwerach wraz ze świadczeniem usług wsparcia technicznego

Warszawa, 2023 r.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

CZĘŚĆ I

I. Definicje.

Pojęcie	Opis
Administrator	Pracownik Zamawiającego odpowiedzialny za zarzadzanie i sprawne działanie Systemu.
Asysta techniczna	Usługa świadczona przez Wykonawcę przez okres łącznego trwania wsparcia technicznego producenta Systemu NDR i Systemu EDR, rozpoczynający się w dniu pierwszego protokolarnego odbioru wdrożenia jednego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego), a kończący się po 12 miesiącach od dnia protokolarnego odbioru wdrożenia kolejnego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego), opisana w OPZ (Część IV rozdział II) oraz postanowieniach umowy.
Awaria krytyczna	Zdarzenie powodujące całkowite unieruchomienie Systemu EDR lub Systemu NDR, uniemożliwiające jego zarządzanie oraz wykorzystywanie.
Błąd	Każde z poniżej opisanych zdarzeń, polegające na: a) znacznym spadku wydajności Systemu NDR lub Systemu EDR; b) niedostępności wybranych funkcjonalności Systemu NDR lub Systemu EDR, istotnych dla Zamawiającego pozwalającej jednak na dalszą realizację ochrony przed atakami; c) braku możliwości korzystania z Systemu NDR lub Systemu EDR, ale uzyskanie oczekiwanych efektów jest możliwe w inny sposób (przez zastosowanie rozwiązania obejściowego).
Czas Reakcji	Czas, jaki upłynie od zgłoszenia w systemie obsługi zgłoszeń serwisowych Awarii krytycznej, Usterki lub Błędu do potwierdzenia rozpoczęcia analizy zgłoszenia i usuwania Awarii krytycznej, Usterki lub Błędu przez służby techniczne Wykonawcy.
Czas Naprawy (rozwiązania)	Czas, jaki upłynie pomiędzy zgłoszeniem Awarii krytycznej, Usterki lub Błędu, a momentem usunięcia Nieprawidłowości w działaniu Systemu przez służby techniczne Wykonawcy tj. usunięcie lub obejście Awarii krytycznej, Usterki lub Błędu zakończonej

	potwierdzeniem usunięcia Nieprawidłowości przez Zamawiającego. Do czasu naprawy nie wlicza się czasu oczekiwania na odpowiedź Zamawiającego.
Dokumentacja	Wszelkie dokumenty sporządzone przez Wykonawcę lub wspólnie przez Strony, w szczególności: Projekt techniczny oraz dokumentacja powykonawczą techniczna wdrożonego Systemu NDR i Systemu EDR.
Dni robocze	Kolejne dni od poniedziałku do piątku za wyjątkiem dni wolnych od pracy zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. Nr 4 poz. 28 z późn. zm.).
Etap	Wyodrębnione części realizacyjne Projektu.
Funkcjonalność	Zdolność Systemu NDR lub Systemu EDR do dostarczenia funkcji zaspokajających potrzeby Zamawiającego.
Godziny eksperckie	Usługa świadczona przez Wykonawcę w ramach prawa opcji, przez okres trwania wsparcia technicznego producenta Systemu NDR i Systemu EDR, rozpoczynający się w dniu pierwszego protokolarnego odbioru wdrożenia jednego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego), a kończący się po 12 miesiącach od dnia protokolarnego odbioru wdrożenia kolejnego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego), opisana w OPZ (Część IV rozdział III) oraz postanowieniach umowy.
Harmonogram	Dokument zawierający terminy realizacji przedmiotu zamówienia w zakresie szczegółowych prac, sporządzony w ramach realizacji Etapu I i Etapu II.
Nieprawidłowość	Wszelkie niezgodności w działaniu Systemu NDR lub Systemu EDR, w tym Usterki, Błędy, Awarie krytyczne.
Projekt	Powiązane ze sobą działania mające na celu realizację przedmiotu zamówienia, w tym Systemu NDR i Systemu EDR.
Projekt techniczny	Dokument opisujący koncepcję funkcjonowania Systemu NDR i Systemu EDR wraz z opisem sposobu realizacji wszystkich wymagań poprzez odpowiednią konfigurację.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

Protokół odbioru częściowego	Dokument potwierdzający dostarczenie i/lub wykonanie określonej części Projektu. Odbiory protokolarne przewidziano dla przedmiotu zamówienia o którym mowa w Części I rozdział III pkt od 2.1.1 do 2.1.5 i pkt od 2.2.1 do 2.2.5.
Protokół odbioru końcowego	Dokument potwierdzający dostarczenie i wykonanie wszystkich wymaganych prac w ramach Projektu, sporządzony po zakończeniu realizacji przedmiotu zamówienia w Etapie I i Etapie II.
Protokół odbioru Zlecenia	Dokument potwierdzający wykorzystanie liczby Roboczogodzin przeznaczonych na prace konsultingowe i utrzymaniowe świadczone przez Wykonawcę w ramach Godzin eksperckich dla Systemów NDR i Systemów EDR.
Roboczogodzina	Jedna godzina zegarowa pracy zespołu Wykonawcy w ramach świadczenia usługi Godzin eksperckich.
System EDR	System zaawansowanej analizy, detekcji i prewencji zagrożeń w stacjach końcowych i serwerach zgodny z wymaganiami funkcjonalnymi opisanymi w Załączniku B oraz niewymaganymi obligatoryjnie wymaganiami opisanymi w Załączniku C, skonfigurowany zgodnie z Projektem technicznym dostarczonym przez Wykonawcę w ramach przedmiotu zamówienia.
System NDR	System zaawansowanej analizy, detekcji i prewencji zagrożeń w ruchu sieciowym zgodny z wymaganiami funkcjonalnymi i pozafunkcjonalnymi opisanymi w Załączniku A, skonfigurowany zgodnie z Projektem technicznym dostarczonym przez Wykonawcę w ramach przedmiotu zamówienia.
Usterka	Niedostępność niektórych funkcjonalności Systemu NDR lub Systemu EDR o mało istotnym dla Zamawiającego znaczeniu lub problem o charakterze ergonomicznym niemającym wpływu na wynik pracy użytkownika oraz wymagane zmiany w konfiguracji Systemu NDR lub Systemu EDR.
Wdrożenie	Opisany zakres działań Wykonawcy mające na celu uruchomienie i konfigurację Systemu NDR lub Systemu EDR.
Wykonawca	Podmiot realizujący umowę.
Zamawiający	Bankowy Fundusz Gwarancyjny z siedzibą w Warszawie

	(ul. ks. I. J. Skorupki 4, 00-546 Warszawa).
Zlecenie	Dokument przekazany Wykonawcy przez Zamawiającego zawierający wniosek o wykonanie określonych usług w ramach świadczenia Godzin eksperckich, opisany w prawie opcji w postanowieniach umowy.

II. Wprowadzenie.

1. Niniejszy dokument opisuje cel, wymagania funkcjonalne i techniczne Zamawiającego dotyczące przedmiotu zamówienia w postępowaniu zakupowym na dostawę, wdrożenie i utrzymanie systemu do analizy, detekcji i prewencji zagrożeń w ruchu sieciowym oraz stacjach końcowych i serwerach dla Bankowego Funduszu Gwarancyjnego.
2. Celem zakupu jest podniesienie poziomu bezpieczeństwa systemu informatycznego BFG.
3. Realizacja Projektu pozwoli uzyskać następujące korzyści:
   - 3.1. Rozszerzenie spektrum widoczności zagrożeń w warstwie sieci komputerowej, stacjach końcowych i serwerach.
   - 3.2. Wykrywanie i przeciwdziałanie propagacji złośliwego oprogramowania w czasie rzeczywistym.
   - 3.3. Zwiększenie możliwości operacyjnych w zakresie obsługi incydentów (detekcji, prewencji, reakcji).
   - 3.4. Odtworzenie śladów i zabezpieczenie materiału dowodowego z incydentu bezpieczeństwa.
   - 3.5. Wsparcie w zakresie identyfikacji podatności w aktywach systemu informatycznego.
   - 3.6. Badanie i ocena wpływu na system informatyczny przetwarzanych plików lub URL nieznanego pochodzenia.
   - 3.7. Optymalizację zarządzania systemami bezpieczeństwa.
   - 3.8. Zwiększenie odporności systemu informatycznego na ataki cybernetyczne.
4. Zamawiający informuje że:
   - 4.1. Infrastruktura teleinformatyczna znajduje się w dwóch połączonych ze sobą centrum przetwarzania danych znajdujących się w dwóch lokalizacjach na terenie Warszawy.
   - 4.2. Styk z siecią Internet realizowany jest za pośrednictwem dwóch operatorów telekomunikacyjnych oraz czterech łączy do Internetu o przepustowości do 1Gb/s przy czym sumaryczny wolumen ruchu nie przekracza 1Gb/s.
   - 4.3. Ruch sieciowy na brzegu sieci Internet (wchodzący i wychodzący) monitorowany jest przez dwa urządzenia brzegowe (zapory sieciowe) Palo Alto. Zapory sieciowe zlokalizowane są w dwóch centrach przetwarzania danych, pracują w klastrze typu active-passive. Awaria aktywnego urządzenia wyzwala przełączenie ruchu z jednoczesnym podtrzymaniem sesji na drugie urządzenie (w innym centrum przetwarzania danych/lokalizacji).
   - 4.4. System ochrony poczty przetwarza dziennie do 3 000 e-mail (nie SPAM) oraz miesięcznie do 30 000 e-mail (nie SPAM).
   - 4.5. System proxy obsługuje dziennie do 1,4 mln żądań http/https kierowanych do sieci Internet.
   - 4.6. W systemie informatycznym pracuje ~1000 urządzeń sieciowych.

5. Wykonawca, a także osoby występujące w jego imieniu podczas realizacji przedmiotu zamówienia, będą zobowiązane do zachowania w tajemnicy wszelkich informacji pozyskanych w związku z przystąpieniem i wykonywaniem zamówienia, w szczególności dotyczących infrastruktury teleinformatycznej Zamawiającego oraz informacji prawnie chronionych. W tym celu każda osoba występująca w imieniu Wykonawcy i biorąca udział w realizacji zamówienia będzie zobowiązana do podpisania zobowiązania o zachowaniu poufności informacji.
6. Użyte w niniejszym dokumencie odniesienia do czasu odpowiadają czasowi środkowoeuropejskiemu.

III. Przedmiot zamówienia.

1. Przedmiotem zamówienia jest dostawa, wdrożenie i utrzymanie Systemu do analizy, detekcji i prewencji zagrożeń w ruchu sieciowym oraz stacjach końcowych i serwerach w Bankowym Funduszu Gwarancyjnym zgodnie z wymaganiami określonymi w niniejszym dokumencie oraz postanowieniach umowy.
2. Przedmiot zamówienia obejmuje:
   - 2.1. W zakresie Systemu NDR:
     - 2.1.1 Wykonanie Projektu technicznego, zawierającego opis koncepcji funkcjonowania Systemu NDR.
     - 2.1.2 Dostawę Systemu NDR, urządzeń wraz z niezbędnymi licencjami do uruchomienia i utrzymania Systemu NDR przez okres min. 12 miesięcy.
     - 2.1.3 Przeprowadzenie min. trzydniowych warsztatów technicznych w zakresie administracji dostarczonym Systemem NDR dla maksymalnie 12 Administratorów Zamawiającego.
     - 2.1.4 Dostosowanie, konfigurację, uruchomienie i przeprowadzenie prac implementacyjno-wdrożeniowych Systemu NDR.
     - 2.1.5 Wykonanie Dokumentacji powykonawczej technicznej uruchomionego Systemu NDR.
     - 2.1.6 Świadczenie serwisu sprzętowego i wsparcia technicznego producenta Systemu NDR przez okres co najmniej 12 miesięcy.
   - 2.2. W zakresie Systemu EDR:
     - 2.2.1. Wykonanie Projektu technicznego, zawierającego opis koncepcji funkcjonowania Systemu EDR.
     - 2.2.2. Dostawę licencji wieczystych typu virtual appliance lub software appliance dla Systemu EDR do ochrony **550** stacji końcowych/serwerów oraz innych wymaganych licencji na oprogramowanie niezbędne do uruchomienia i utrzymania systemu przez okres min. 12 miesięcy.

2.2.3. Przeprowadzenie min. dwudniowych warsztatów technicznych w zakresie instalacji i administracji dostarczonym Systemem EDR dla maksymalnie 12 Administratorów Zamawiającego.

2.2.4. Dostosowanie, konfigurację, uruchomienie i przeprowadzenie prac implementacyjno-wdrożeniowych Systemu EDR.

2.2.5. Wykonanie Dokumentacji powykonawczej technicznej uruchomionego Systemu EDR.

2.2.6. Świadczenie usług wsparcia technicznego producenta Systemu EDR przez okres 12 miesięcy.

2.3. Zapewnienie świadczenia usługi Asysty technicznej przez Wykonawcę dla Systemu EDR i Systemu NDR.

2.4. Zapewnienie świadczenia usługi Godzin eksperckich przez Wykonawcę dla Systemu EDR i Systemu NDR.

3. Zakres realizacji przedmiotu zamówienia oraz szczegółowe wymagania konieczne do spełnienia przez Wykonawcę dla:

3.1. Systemu NDR zostały opisane w Części II (wymagania: ogólne, w zakresie wdrożenia, w zakresie testów akceptacyjnych, w zakresie warsztatów technicznych, funkcjonalne i pozafunkcjonalne) i Części IV (wymagania w zakresie wsparcia technicznego producenta i Asysty technicznej i Godzin eksperckich).

3.2. Systemu EDR zostały opisane w Części III (wymagania: ogólne, w zakresie wdrożenia, w zakresie testów akceptacyjnych, w zakresie warsztatów technicznych, funkcjonalne) i Części IV (wymagania w zakresie wsparcia technicznego producenta, Asysty technicznej i Godzin eksperckich).

4. Wykonanie przedmiotu zamówienia o którym mowa w punktach od 2.1.1 do 2.1.5 oraz od 2.2.1 do 2.2.5 będzie potwierdzone stosownym Protokołem odbioru częściowego dla każdej zakończonej części. Całościowe wykonanie przedmiotu zamówienia zostanie potwierdzone Protokołem odbioru końcowego, oddzielnie dla każdego z systemów.

5. Wykonanie przedmiotu zamówienia o którym mowa w punkcie 2.4 będzie potwierdzone Protokołem odbioru Zlecenia wykonanej usługi, rozliczanej w okresie 3 miesięcznym.

6. Bieg okresu serwisu sprzętowego i wsparcia technicznego producenta dla Systemu NDR rozpoczyna się od dnia przekazania do użytkowania przedmiotu zamówienia o którym mowa w pkt 2.1.4 potwierdzonego Protokołem odbioru częściowego z wdrożenia.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

7. Bieg okresu wsparcia technicznego producenta dla Systemu EDR rozpoczyna się od dnia przekazania do użytkowania przedmiotu zamówienia o którym mowa w pkt 2.2.4 potwierdzonego Protokołem odbioru częściowego z wdrożenia.

IV. Terminy i etapy realizacji.

1. Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 100 Dni roboczych, liczonym od dnia zawarcia umowy.
2. W terminie do 15 Dni roboczych od daty zawarcia umowy Wykonawca uzgodni i przedstawi zamawiającemu do akceptacji Harmonogram realizacji przedmiotu zamówienia w zakresie Systemu EDR i Systemu NDR.
3. Harmonogram musi zawierać plan prac, opisywać terminy poszczególnych zadań. Plan prac powinien być konsultowany z Zamawiającym, tak aby odzwierciedlał realne potrzeby i możliwości Zamawiającego. W ramach spotkań roboczych Wykonawca zobowiązany jest do przedstawienia planu i uwzględnienia uwag Zamawiającego co do zakresu i formy realizacji planu.
4. Przedmiot zamówienia zostanie zrealizowany w trzech etapach:

3.1. **Etap I – System NDR (dostawa, wdrożenie i warsztaty):**

3.1.1. Wykonawca przygotuje opis niezbędnych prac w celu wdrożenia Systemu NDR wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającym i Wykonawcą w modelu RACI.

3.1.2. Wykonawca przedstawi listę pracowników odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi (adres e-mail, nr tel.).

3.1.3. Wykonawca dostarczy sprzęt i przekaże wymagane licencje/subskrypcje umożliwiające przystąpienie do wdrożenia.

3.1.4. Wdrożenie oraz przeprowadzenie warsztatów zakresie dostarczonego Systemu NDR:

a) Omówienie planu działania podczas realizacji Projektu, w tym Wdrożenia Systemu NDR oraz uszczegółowienie Harmonogramu prowadzenia prac.

b) Przekazanie dokumentacji technicznej udostępnionej przez producenta oferowanego Systemu NDR (dopuszcza się dokumentację techniczną w języku angielskim).

c) Opracowanie i dostarczenie Projektu technicznego dla Systemu NDR.

d) Opracowanie planu testów akceptacyjnych, zawierających min. zdefiniowany zakres i cele przeprowadzenia testów akceptacyjnych, scenariusze testowe, wykaz czynności niezbędnych do wykonania wraz z podziałem odpowiedzialności pomiędzy Wykonawcę

i Zamawiającego, ustalone kryteria akceptacji testów, opis klasyfikacji wykrytych Nieprawidłowości, opis zasad naprawy wykrytych Nieprawidłowości Systemu NDR, opis zasad sporządzenia raportu z przeprowadzonych testów akceptacyjnych.

e) Opracowanie materiałów na warsztaty z Systemu NDR dla Administratorów Zamawiającego.
f) Przeprowadzenie warsztatów dla Administratorów Zamawiającego zgodnie z opisem w Części II rozdział IV - „Wymagania w zakresie warsztatów technicznych dla Systemu NDR".
g) Przygotowanie propozycji konfiguracji inspekcji ruchu SSL/TLS na urządzeniach brzegowych Zamawiającego (Palo Alto seria PA-3200) oraz przekazywania ruchu na sondy sieciowe.
h) Przygotowanie propozycji konfiguracji urządzeń Systemu NDR.
i) Instalacja urządzeń w lokalizacji Zamawiającego i integracja z systemem informatycznym BFG.
j) Konfiguracja Systemu NDR oraz wymaganych do wdrożenia elementów infrastruktury sieciowej, w tym konfiguracja Network Packet Broker na zaporze sieciowej Zamawiającego i podłączenie sondy sieciowej do łańcucha zabezpieczeń.
k) Implementacja zaprojektowanych polityk, raportów i reguł korelacyjnych.
l) Dobór odpowiednich parametrów celem otrzymania najwydajniejszej i najbardziej bezpiecznej konfiguracji Systemu NDR.
m) Przeprowadzenie prac optymalizacji Systemu NDR pod kątem minimalizacji liczby fałszywych alertów.
n) Przeprowadzenie testów poprawności instalacji i konfiguracji Systemu NDR.
o) Przygotowanie szablonów powiadomień w przypadku wykrycia incydentu bezpieczeństwa.
p) Przygotowanie procedur utrzymaniowych Systemu NDR.
q) Wykonanie technicznej dokumentacji powykonawczej.
r) Produkcyjne uruchomienie Systemu NDR.
s) Przygotowanie raportu z wdrożenia Systemu NDR.

3.2. **Etap II – System EDR (dostawa, wdrożenie i warsztaty):**

3.2.1. Wykonawca przygotuje opis niezbędnych prac w celu wdrożenia Systemu EDR wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającym i Wykonawcą w modelu RACI.

3.2.2. Wykonawca przedstawi listę pracowników odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi (adres e-mail, nr tel.).

3.2.3. Wykonawca dostarczy i przekaże wymagane licencje/subskrypcje umożliwiające przystąpienie do wdrożenia.

3.2.4. Wdrożenie oraz przeprowadzenie warsztatów w zakresie dostarczonego Systemu EDR:

a) Omówienie planu działania podczas realizacji Projektu, w tym Wdrożenia Systemu EDR oraz uszczegółowienie Harmonogramu prowadzenia prac.

b) Wykonanie analizy przedwdrożeniowej.

c) Opracowanie i dostarczenie Projektu technicznego.

d) Opracowanie planu testów akceptacyjnych, zawierających min. zdefiniowany zakres i cele przeprowadzenia testów akceptacyjnych, scenariusze testowe, wykaz czynności niezbędnych do wykonania wraz z podziałem odpowiedzialności pomiędzy Wykonawcę i Zamawiającego, ustalone kryteria akceptacji testów, opis klasyfikacji wykrytych Nieprawidłowości, opis zasad naprawy wykrytych Nieprawidłowości Systemu EDR, opis zasad sporządzenia raportu z przeprowadzonych testów akceptacyjnych.

e) Opracowanie materiałów na warsztaty dla Administratorów Zamawiającego.

f) Przeprowadzenie warsztatów dla Administratorów Zamawiającego zgodnie z opisem w Części III, rozdział IV - „Wymagania w zakresie warsztatów technicznych dla Systemu EDR".

g) Przygotowanie propozycji konfiguracji.

h) Instalacja niezbędnych komponentów do uruchomienia Systemu EDR.

i) Konfiguracja Systemu EDR (w tym integracja z usługami katalogowymi Zamawiającego).

j) Implementacja zaprojektowanych polityk, raportów i reguł.

k) Dobór odpowiednich parametrów celem otrzymania najwydajniejszej i najbardziej bezpiecznej konfiguracji Systemu EDR.

l) Przeprowadzenie prac optymalizacji Systemu EDR pod kątem minimalizacji liczby fałszywych alertów.

m) Przeprowadzenie testów poprawności instalacji i konfiguracji Systemu EDR.

n) Przygotowanie szablonów powiadomień dla przypadku wykrycia incydentu bezpieczeństwa.

o) Przygotowanie procedur utrzymaniowych Systemu EDR.
p) Wykonanie dokumentacji powykonawczej technicznej.
q) Produkcyjne uruchomienie Systemu EDR.
r) Przygotowanie raportu z Etapu II.

3.3. **Etap III – Zapewnienie usługi wsparcia technicznego, Asysty technicznej i Godzin eksperckich dla Systemu NDR, Systemu EDR.**

Realizacja usług zgodnie z wymaganiami określonymi w Części IV rozdział I-III.

CZĘŚĆ II

I. Wymagania ogólne dla Systemu NDR.

1. Komponenty Systemu NDR muszą być dostarczone, instalowane i zintegrowane z infrastrukturą teleinformatyczną Zamawiającego.
2. Wszystkie licencje niezbędne do realizacji przedmiotu zamówienia dostarcza Wykonawca bez dodatkowych opłat w ramach przewidzianego wynagrodzenia. Licencje powinny zapewnić obsługę łącznego ruchu do 1 Gbit/s. Licencje będą posiadały minimum 12 miesięczne wsparcie techniczne producenta Systemu NDR (maintenance).
3. System NDR musi składać się co najmniej z poniższych głównych komponentów dostarczonych w formie sprzętowej (appliance):
   3.1. Urządzenia zarządzającego – urządzenia do zarządzania Systemem NDR i analizy zdarzeń.
   3.2. Sondy sieciowej (2 sztuki o tych samych parametrach) – urządzenia analizującego ruch sieciowy na styku sieci z siecią Internet, której zadaniem jest inspekcja ruchu sieciowego na wszystkich portach TCP/UDP.
   3.3. Sondy pocztowej (2 sztuki o tych samych parametrach) – urządzenia zapewniającego inspekcję poczty elektronicznej e-mail.
   3.4. Piaskownicy – urządzenia umożliwiającego „detonację" plików nieznanego pochodzenia lub adresów URL w izolowanym środowisku.
   3.5. Magazynu sieciowego – urządzenia agregującego informacje opisującego przepływ ruchu sieciowego i obiekty przesyłane przy użyciu szerokiej gamy protokołów w sposób nieselektywny. Komponent powinien działać przynajmniej w oparciu o gromadzenie rozbudowanych metadanych opisujących transmisje sieciowe, przesyłane pliki, elementy

składowe plików, własności protokołów i transmisji, a także w oparciu o dane przesyłane z sond.

4. Całość dostarczanego sprzętu musi być fabrycznie nowa, nieużywana we wcześniejszych projektach i wyprodukowana w okresie do 6 miesięcy przed datą dostarczenia Zamawiającemu.
5. Dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na gwarancji świadczonej przez producenta sprzętu przez okres nie krótszy niż 12 miesięcy (zgodnie z przestawioną ofertą Wykonawcy).
7. Zgłoszenia serwisowe w ramach gwarancji musza być przyjmowane 24 godz. w każdym dniu tygodnia.
8. Wszelkie naprawy sprzętowe w ramach gwarancji będą realizowane w siedzibie Zamawiającego (on-site).
9. Dostarczony sprzęt będzie zakupiony w autoryzowanym kanale sprzedaży producenta na rynek Unii Europejskiej a serwis gwarancyjny musi być autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.
10. Wykonawca najpóźniej w dniu dostawy sprzętu złoży stosowne oświadczenie producenta urządzeń i oprogramowania, że w przypadku niewywiązywania się z obowiązków gwarancyjnych Wykonawcy, producent dostarczonych urządzeń i oprogramowania przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym.
11. Zamawiający wymaga dołączenia do urządzeń instrukcji obsługi w języku polskim lub angielskim (w wersji elektronicznej nadającej się do samodzielnego wydruku lub drukowanej).
12. Dostarczone urządzenia musza być ze sobą kompatybilne w zakresie zapewniającym osiągnięcie wymaganej funkcjonalności.
13. Urządzenia muszą posiadać parametry takie jak opisane w szczegółowej specyfikacji dostępnej na stronie producenta.
14. System NDR musi być dostosowany i dostrojony do istniejącej sieci teleinformatycznej Zamawiającego oraz wyskalowany do przetwarzania założonego wolumenu ruchu Zamawiającego (min. 1Gb/s).
15. System NDR musi umożliwiać przechowywanie metadanych ruchu sieciowego do analizy przez przynajmniej 90 dni.
16. Wszystkie zaoferowane główne komponenty stanowiące System NDR muszą być kompatybilne. W przypadku zaoferowania komponentów różnych producentów Wykonawca zobowiązany jest złożyć

oświadczenie wraz z ofertą, że sprzęt jest kompatybilny z oferowanymi pozostałymi elementami Systemu oraz gwarantuje poprawność i stabilność pracy całego Systemu NDR.

17. System NDR musi być dostosowany do pracy ciągłej tj. 24 godziny na dobę, 7 dni w tygodniu, przez 365 dni w roku.
18. Wszystkie komponenty Systemu NDR muszą być zarządzane z jednej centralnej konsoli.

II. Wymagania w zakresie wdrożenia Systemu NDR.

1. Wdrożenie Systemu NDR będzie realizowane w siedzibie Zamawiającego, tj. ul. ks. I. J. Skorupki 4, 00-546 Warszawa oraz lokalizacji zapasowej znajdującej się na terenie Warszawy.
2. Wykonawca zobowiązuje się do przestrzegania wewnętrznych procedur oraz regulaminów obowiązujących osoby przebywające w siedzibie Zamawiającego, o których Wykonawca zostanie poinformowany. Pracownicy Wykonawcy zobowiązani są do podpisania oświadczenia o zachowaniu poufności. Wykonawca zobowiązuje się do poinformowania swoich pracowników (współpracowników) o wewnętrznych procedurach oraz regulaminach obowiązujących u Zamawiającego. Zamawiający zastrzega sobie prawo do ograniczenia dostępu do pomieszczeń Zamawiającego dla osób, które nie przestrzegają wewnętrznych procedur oraz regulaminów obowiązujących u Zamawiającego. Zamawiający nie ponosi negatywnych skutków ograniczenia dostępności dla takich osób.
3. Wykonawca powinien skonfigurować System NDR zgodnie z Projektem technicznym zatwierdzonym przez Zamawiającego.
4. Wykonawca podczas przygotowania Projektu i jego realizacji musi uwzględnić specyfikę struktury organizacyjnej Zamawiającego.
5. Projekt techniczny musi zawierać min.:
   5.1. Schemat architektury rozwiązania, jego organizację, oraz wszystkie funkcje przewidziane do realizacji przez System NDR.
   5.2. Wykaz dostarczanego oprogramowania, licencji i sprzętu niezbędnego do poprawnej pracy Systemu NDR.
   5.3. Zasady i plany instalacji, uruchomienia i wdrożenia Systemu NDR.
   5.4. Wskazywać punkty krytyczne i zagrożenia mające wpływ na niezawodne działanie Systemu.
   5.5. Opracowanie kluczowych wskaźników efektywności KPI (key performance indicator) dla dostarczanego Systemu NDR. Wskaźniki muszą przedstawiać źródło i zakres badanych danych, metodę pomiaru, proponowaną częstotliwość pomiaru.

6. Dokumentacja techniczna powykonawcza musi zawierać opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację Systemu, a w szczególności:
   6.1. Opis architektury technicznej.
   6.2. Wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych.
7. Projekt techniczny i dokumentacja powdrożeniowa powinny charakteryzować się wysoką jakością wykonania, być czytelne i zrozumiałe oraz sporządzone w języku polskim.
8. System NDR zostanie zainstalowany we wskazanych przez Zamawiającego pomieszczeniach i miejscach w dwóch centrach przetwarzania danych (podstawowym i zapasowym). W zapasowym centrum przetwarzania danych zostaną umieszczone jedynie dwie sondy: sieciowa i pocztowa. Pozostała infrastruktura Systemu NDR będzie zainstalowana w podstawowym centrum przetwarzania danych. Urządzenia wchodzące w skład Systemu NDR zostaną zamontowane w szafach telekomunikacyjnych i podłączone za pomocą stosownych przewodów, w tym przewodów zasilających.
9. Wykonawca dokona połączeń kablowych, w tym połączeń poprzez istniejące okablowanie strukturalne. Pracownicy Zamawiającego wskażą stosowne do podłączenia porty przełączników sieciowych.
10. System NDR i wszystkie wymagane urządzanie zostaną dostarczone do siedziby Zamawiającego na własny koszt i ryzyko Wykonawcy.
11. Pracownicy Zamawiającego w asyście Wykonawcy dokonają konfiguracji rozszywania ruchu SSL/TLS na dwóch urządzeniach brzegowych (seria PA-3200) pracującym w klastrze w trybie active-passive oraz/lub na przełącznikach sieciowych Zamawiającego oraz wykreują przekazywanie ruchu sieciowego do analizy na sondę sieciową.
12. Sonda pocztowa Systemu NDR musi współpracować z systemem pocztowym i systemem ochrony poczty używanym przez Zamawiającego.
13. Pracownicy Zamawiającego w asyście Wykonawcy dokonają rekonfiguracji sposobu dostarczania i wysyłania poczty elektronicznej w odpowiednich systemach, w sposób umożliwiający umieszczenie sondy pocztowej (MTA) w łańcuchu zabezpieczeń.
14. System NDR musi być w pełni zintegrowany z dotyczącą go infrastrukturą Zamawiającego.
15. Wykonawca wykona aktualizację oprogramowania układowego oraz mikrokodów (firmware) dostarczonych urządzeń do najnowszej lub wskazanej przez Zamawiającego wersji oprogramowania opublikowanego przez producenta na dzień dostawy sprzętu.

16. Sposób działania sond nie może mieć wpływu na ciągłość działania monitorowanych przez nie sieci. W szczególności awaria sondy wpiętej in-line nie może powodować niedostępności usług sieciowych.
17. System NDR powinien zapewniać integrację z usługami katalogowymi Zamawiającego w zakresie autoryzacji użytkowników w celu identyfikacji użytkownika przesyłającego określone dane.
18. System NDR musi umożliwiać przechowywanie metadanych ruchu sieciowego do analizy przez przynajmniej 90 dni oraz archiwizację alertów z materiałem dowodowym w zakresie zdarzeń sieciowych i incydentów bezpieczeństwa na zewnętrznym zasobie sieciowym przez przynajmniej 12 miesięcy. (Zamawiający zapewni odpowiednią przestrzeń dla archiwum alertów).
19. Wykonawca dokona sprawdzenia poprawności działania Systemu NDR. Wykonawca musi przygotować scenariusze testowe i przeprowadzić testy, na których podstawie zostanie dokonany odbiór wdrożenia i przedstawić do akceptacji Zamawiającemu.
20. Wszelkie niezbędne testy w celu weryfikacji poprawności instalacji i konfiguracji Systemu NDR muszą zostać przeprowadzone zgodnie z wymaganiami przedstawionymi w Części II rozdziale III - „Wymagania w zakresie testów akceptacyjnych Systemu NDR".
21. Wykonawca po uzyskaniu wyników pozytywnych z przeprowadzonych testów dokona uruchomienia produkcyjnego wdrożonego Systemu NDR.
22. Wykonawca musi uruchomić interfejs zarządzania Systemem NDR.
23. Przygotowanie procedur utrzymaniowych Systemu NDR.
24. Przeprowadzenie certyfikowanych warsztatów z użytkowania i administracji wdrożonego Systemu dla Administratorów Systemu NDR musi odbyć się przed wdrożeniem produkcyjnym, podczas realizacji Etapu I.
25. Wykonawca powinien sporządzić powykonawczą dokumentację techniczną uruchomionego Systemu NDR i przekazać ją do Zamawiającego do dnia zakończenia Etapu I.
26. Przygotowanie raportu z wdrożenia przedmiotu zamówienia w zakresie Systemu NDR.
27. Zamawiający może w trakcie realizacji Wdrożenia korzystać z usług osób trzecich w celu kontroli jakości i sposobu prowadzenia całości Projektu lub poszczególnych jego części. Wykonawca będzie zobowiązany do udzielenia takim osobom wszelkich informacji, danych lub wyjaśnień dotyczących realizacji wdrożenia.
28. W trakcie realizacji Projektu Wykonawca będzie stosował metodykę zarządzania projektami PRINCE2 lub równoważną spełniając tym samym wymagania zawarte w tym rozdziale. W uzasadnionych przypadkach, za zgodą Zamawiającego dopuszczalne jest stosowanie innej metodyki zarządzania projektami.

III. Wymagania w zakresie testów akceptacyjnych dla Systemu NDR.

1. Wykonawca opracuje plan i harmonogram testów akceptacyjnych, który wymaga akceptacji ze strony Zamawiającego.
2. Wykonawca opracuje scenariusze testowe zawierające m.in.:
   2.1. Listę wymagań, które dany scenariusz realizuje.
   2.2. Zestawy danych wejściowych dla testów.
   2.3. Listę kroków w przebiegu testu.
   2.4. Opis pożądanego rezultatu testu.
3. Zamawiający, w ramach procesu weryfikacji planu testów przygotowanego przez Wykonawcę, będzie miał prawo zgłaszania własnych scenariuszy testów.
4. Zostaną wykonane następujące elementy testów i odbioru:
   4.1. Testy wykrywania i ochrony przed złośliwym oprogramowaniem.
   4.2. Testy wykrywania i ochrony przed zagrożeniami Advanced Persistent Threat (APT).
   4.3. Testy wykrywania i ochrony przed wyciekiem danych.
   4.4. Testy ochrony przed cyberatakami w czasie rzeczywistym.
   4.5. Test polityk.
   4.6. Testy obciążeniowe.
   4.7. Testy wydajnościowe.
   4.8. Zgodność konfiguracji sprzętowej urządzeń z zamówieniem.
   4.9. Testy zarządzania konfiguracją i politykami za pomocą centralnego modułu zarządzania.
5. Za przeprowadzenie testów odpowiedzialny jest Wykonawca. Osoby wskazane przez Zamawiającego będą współuczestniczyły i nadzorowały przeprowadzane testy akceptacyjne.
6. Testy wydajnościowe muszą symulować standardowy i szczytowy ruch sieciowy.
7. Wyniki testów wydajnościowych muszą być powtarzalne.
8. Z przeprowadzonych testów zostanie przedstawiony raport.
9. Testy akceptacyjne zostaną przeprowadzone na wdrożonym Systemie NDR.
10. Każda niezgodność pomiędzy oczekiwanym wynikiem testu, a wynikiem otrzymanym podczas wykonywania testu, stanowi podstawę do zgłoszenia Nieprawidłowości.
11. W przypadku wykrycia Nieprawidłowości Zamawiający ma prawo do wstrzymania testów do czasu wprowadzenia odpowiedniej poprawki Systemu NDR.
12. Wykonawca zobowiązany jest do usunięcia wszystkich Nieprawidłowości wykrytych w Systemie NDR podczas przeprowadzania testów akceptacyjnych w czasie ustalonym z Zamawiającym.

13. Zamawiający ma obowiązek wykonania testów poprawności przekazanego rozwiązania wykrytej Nieprawidłowości, a w przypadku negatywnej weryfikacji ma prawo żądać ponownego rozwiązania zgłoszonej Nieprawidłowości.

IV. Wymagania w zakresie warsztatów technicznych dla Systemu NDR.

1. Wykonawca przeprowadzi autoryzowane przez producenta warsztaty techniczne dla maks. 12 Administratorów Zamawiającego obejmujące min. zagadnienia:
   1.1. Instalacji agentów i konfiguracji Systemu NDR.
   1.2. Administracji Systemem pozwalającą na samodzielne budowanie nowych polityk bezpieczeństwa, tworzenie własnych szablonów raportów, powiadomień/alarmów, przeszukiwania i grupowania zdarzeń, reguł korelacji, wyszukiwania i filtrowania, itd.
2. Warsztaty techniczne muszą rozpocząć się przed wdrożeniem Systemu NDR, nie wcześniej niż 15 Dni roboczych przed zaplanowaną datą wdrożenia.
3. Warsztaty muszą trwać min. 3 dni, w sumie nie mniej niż 18 godzin.
4. Warsztaty muszą być przeprowadzone w dwóch terminach ustalonych przez strony.
5. Warsztaty muszą być przeprowadzone w języku polskim. Cena oferowanych warsztatów musi obejmować pełne koszty ich przeprowadzenia, w szczególności koszty materiałów szkoleniowych, podróży, zakwaterowania, wyżywienia uczestników. Warsztaty odbędą się w miejscu wskazanym przez Wykonawcę. Wymagana jest akceptacja miejsca przez Zamawiającego.
6. Po zakończeniu warsztatów Administrator Systemu NDR będzie potrafił m.in.:
   6.1. Administrować wszystkimi komponentami Systemu NDR.
   6.2. Dokonywać konfiguracji Systemu NDR wg aktualnych potrzeb działu IT, w tym konfigurowania polityk retencji zdarzeń.
   6.3. Definiować kryteria przeszukiwania zapisanych informacji o analizowanym ruchu przez budowanie złożonych filtrów.
   6.4. Dodawać nowe polityki bezpieczeństwa.
   6.5. Tworzyć i modyfikować istniejące szablony raportów.
   6.6. Przeszukiwać, filtrować i grupować alerty według dostępnych w Systemie NDR kryteriów.
   6.7. Tworzyć reguły korelacyjne dla zaistniałych w ruchu sieciowym zdarzeń.
7. Wykonawca ma obowiązek zapewnić wykładowców posiadających odpowiednie kwalifikacje zawodowe i niezbędną wiedzę fachową w zakresie tematyki warsztatów potwierdzoną certyfikatem z oferowanej technologii wystawionym przez producenta wdrażanego rozwiązania.

8. Wykonawca dostarczy materiały warsztatowe uczestnikom warsztatów w formie elektronicznej w formacie ogólnie dostępnym umożliwiającym drukowanie oraz w formie papierowej na co najmniej 2 Dni robocze przed terminem rozpoczęcia warsztatów.
9. Wykonawca przygotuje i przekaże Administratorom Zamawiającego uczestniczącym w warsztatach imienne certyfikaty uczestnictwa.

V. Wymagania funkcjonalne i pozafunkcjonalne dla Systemu NDR.

System NDR musi spełniać wszystkie wymagania funkcjonalne oraz pozafunkcjonalne o których mowa w załączniku nr A.

CZĘŚĆ III

I. Wymagania ogólne dla Systemu EDR.

1. System EDR musi być dostarczony, zainstalowany w infrastrukturze teleinformatycznej Zamawiającego.
2. System EDR musi zapewniać ochronę **550** stacji końcowych/serwerów.
3. Wszystkie licencje[1] (wieczyste typu virtual appliance lub software appliance) niezbędne do realizacji przedmiotu zamówienia dostarcza Wykonawca bez dodatkowych opłat w ramach przewidzianego wynagrodzenia. Licencje dla Systemu EDR będą posiadały 12 miesięczne wsparcie techniczne producenta (maintenance).
4. Zamawiający wymaga aby dostarczone licencje po wygaśnięciu nie spowodowały zatrzymania działania Systemu EDR i nie ograniczą po tym czasie jego funkcjonalności pomimo wstrzymania możliwości pobierania aktualizacji i nowych sygnatur.
5. System EDR musi być odpowiednio wyskalowany wydajnościowo do obsługi 15% więcej klientów niż zakłada zamówienie.
6. System EDR musi umożliwić przechowywanie zdarzeń przez co najmniej 120 dni.
7. System EDR musi składać się co najmniej z poniższych komponentów:
   6.1. Konsoli zarządzającej – systemu do zarządzania Systemem EDR i analizy zdarzeń.
   6.2. Agenta – oprogramowania klienckiego dla systemów MS Windows, Mac i Linux instalowanego na stacjach końcowych i serwerach.
   6.3. Serwera danych – systemu przechowującego co najmniej informacje o zdarzeniach zainstalowanego na serwerze Windows oraz/lub Linux.
7. System EDR musi być dostosowany do pracy ciągłej tj. 24 godziny na dobę, 7 dni w tygodniu, przez 365 dni w roku.

II. Wymagania w zakresie wdrożenia Systemu EDR.

1. Wdrożenie Systemu EDR będzie realizowane w siedzibie Zamawiającego, tj. ul. ks. I. J. Skorupki 4, 00-546 Warszawa.

[1] Zamawiający zapewni zasoby sprzętowe dla Systemu EDR w ramach posiadanego środowiska VMWARE. Zamawiający posiada licencję na system operacyjny MS Windows DataCenter 2016/2019/2022 i licencje dostępowe CAL. Licencje na dodatkowe oprogramowanie (inne OS, baza danych) zapewnia Wykonawca zgodnie z rekomendacjami producenta Systemu EDR. Dostarczone licencje mają zapewnić możliwość przejścia w tryb failover w razie awarii (przeniesienie maszyn wirtualnych wchodzących w skład Systemu EDR na inny węzeł klastra)

2. System EDR ma być dostarczony w modelu „on premise", czyli musi być zainstalowany w infrastrukturze Zamawiającego.
3. Wykonawca zobowiązuje się do przestrzegania wewnętrznych procedur oraz regulaminów obowiązujących osoby przebywające w siedzibie Zamawiającego, o których Wykonawca zostanie poinformowany. Pracownicy Wykonawcy zobowiązani są do podpisania oświadczenia o zachowaniu poufności. Wykonawca zobowiązuje się do poinformowania swoich pracowników (współpracowników) o wewnętrznych procedurach oraz regulaminach obowiązujących u Zamawiającego. Zamawiający zastrzega sobie prawo do ograniczenia dostępu do pomieszczeń Zamawiającego dla osób, które nie przestrzegają wewnętrznych procedur oraz regulaminów obowiązujących u Zamawiającego. Zamawiający nie ponosi negatywnych skutków ograniczenia dostępności dla takich osób.
4. Wykonawca wykona analizę przedwdrożeniową infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem EDR, potrzeb użytkownika i wymagań funkcjonalnych odnośnie konfiguracji Systemu EDR, której wynikiem będzie Projekt Techniczny.
5. Wykonawca powinien skonfigurować System EDR zgodnie Projektem technicznym zatwierdzonym przez Zamawiającego.
6. Projekt techniczny musi zawierać min.:
   6.1. Schemat architektury rozwiązania, jego organizację oraz wszystkie funkcje przewidziane do realizacji przez System EDR.
   6.2. Wykaz oprogramowania, licencji dostarczonych i niezbędnych do poprawnej pracy Systemu EDR.
   6.3. Wymogi takie jak ilość urządzeń maszyn wirtualnych wraz z dodatkowymi parametrami jak vCPU, vRAM, vHDD koniecznymi do obsługi wszystkich składowych Systemu EDR.
   6.4. Zasady i plany instalacji, uruchomienia i wdrożenia Systemu EDR.
   6.5. Wskazywać punkty krytyczne i zagrożenia mające wpływ na niezawodne działanie Systemu EDR.
   6.6. Opracowanie kluczowych wskaźników efektywności KPI (key performance indicator) dla dostarczanego Systemu EDR. Wskaźniki muszą przedstawiać źródło i zakres badanych danych, metodę pomiaru, proponowaną częstotliwość pomiaru.
7. Dokumentacja techniczna powykonawcza musi zawierać opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację Systemu EDR, a w szczególności:
   7.1. Opis architektury technicznej.

7.2. Wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych.

8. Projekt techniczny i dokumentacja powdrożeniowa powinny charakteryzować się wysoką jakością wykonania, być czytelne i zrozumiałe oraz sporządzone w języku polskim.
9. System EDR musi być w pełni zintegrowany z dotyczącą go infrastrukturą Zamawiającego (integracja z usługami katalogowymi Zamawiającego w zakresie autoryzacji użytkowników w celu identyfikacji).
10. System EDR musi umożliwiać przechowywanie zdarzeń przez przynajmniej 120 dni.
11. System EDR zostanie zainstalowany we wskazanych przez Zamawiającego pomieszczeniach oraz wskazanych przez Zamawiającego miejscach w siedzibie Zamawiającego.
12. Wykonawca dokona wdrożenia poprzez instalację i konfigurację potrzebnej infrastruktury serwerowej Systemu EDR oraz uruchomi agentów Systemu EDR na co najmniej 100 stacjach klienckich i/lub serwerach, które wskaże Zamawiający. Instalacja agentów na pozostałe urządzenia zostanie dokonana przez personel Zamawiającego przy użyciu przygotowanych przez Wykonawcę tzw. paczek instalacyjnych, umożliwiających masową instalację łącznie **550** agentów. Wykonawca będzie zobowiązany do pomocy w propagacji oraz konsultacji w ramach Asysty technicznej po wdrożeniu.
13. Wykonawca dokona sprawdzenia poprawności działania Systemu EDR. Wykonawca musi przygotować scenariusze testowe i przeprowadzić testy, na których podstawie zostanie dokonany odbiór wdrożenia i przedstawić do akceptacji Zamawiającemu.
14. Wszelkie niezbędne testy w celu weryfikacji poprawności instalacji i konfiguracji Systemu EDR muszą zostać przeprowadzone zgodnie z wymaganiami przedstawionymi w Części III, rozdział III - „Wymagania w zakresie testów akceptacyjnych dla Systemu EDR".
15. Wykonawca po uzyskaniu wyników pozytywnych z przeprowadzonych testów dokona uruchomienia produkcyjnego wdrożonego Systemu EDR.
16. Przeprowadzenie warsztatów z użytkowania i administracji wdrożonego rozwiązania EDR dla Administratorów Systemu musi odbyć się przed wdrożeniem produkcyjnym podczas realizacji Etapu II.
17. Wykonawca powinien sporządzić dokumentację powykonawczą techniczną uruchomionego Systemu EDR i przekazać ją do Zamawiającego do dnia zakończenia Etapu II.
18. Zamawiający może w trakcie realizacji Wdrożenia korzystać z usług osób trzecich w celu kontroli jakości i sposobu prowadzenia całości Projektu lub poszczególnych jego części. Wykonawca będzie

zobowiązany do udzielenia takim osobom wszelkich informacji, danych lub wyjaśnień dotyczących realizacji wdrożenia.

19. W trakcie realizacji Projektu Wykonawca będzie stosował metodykę zarządzania projektami PRINCE2 lub równoważną spełniając tym samym wymagania zawarte w tym rozdziale. W uzasadnionych przypadkach, za zgodą Zamawiającego dopuszczalne jest stosowanie innej metodyki zarządzania projektami.

III. Wymagania w zakresie testów akceptacyjnych dla Systemu EDR.

1. Wykonawca opracuje plan i harmonogram testów akceptacyjnych, który wymaga akceptacji ze strony Zamawiającego.
2. Za przeprowadzenie testów odpowiedzialny jest Wykonawca. Osoby wskazane przez Zamawiającego będą współuczestniczyły i nadzorowały przeprowadzane testy akceptacyjne.
3. Zamawiający, w ramach procesu weryfikacji planu testów przygotowanego przez Wykonawcę, będzie miał prawo zgłaszania własnych scenariuszy testów.
4. Z przeprowadzonych testów zostanie przedstawiony raport.
5. Testy akceptacyjne zostaną przeprowadzone na wdrożonym Systemie EDR.
6. Każda niezgodność pomiędzy oczekiwanym wynikiem testu, a wynikiem otrzymanym podczas wykonywania testu, stanowi podstawę do zgłoszenia Nieprawidłowości.
7. W przypadku wykrycia Nieprawidłowości Zamawiający ma prawo do wstrzymania testów do czasu wprowadzenia odpowiedniej poprawki Systemu EDR.
8. Wykonawca zobowiązany jest do usunięcia wszystkich Nieprawidłowości wykrytych w Systemie EDR podczas przeprowadzania testów akceptacyjnych w czasie ustalonym z Zamawiającym.
9. Zamawiający ma obowiązek wykonania testów poprawności przekazanego rozwiązania wykrytej Nieprawidłowości, a w przypadku negatywnej weryfikacji ma prawo żądać ponownego rozwiązania zgłoszonej Nieprawidłowości.

IV. Wymagania w zakresie warsztatów technicznych dla Systemu EDR.

1. Wykonawca przeprowadzi autoryzowane przez producenta warsztaty techniczne dla maks. 12 Administratorów Zamawiającego obejmujące min. zagadnienia:
   1.1. Instalacji i konfiguracji Systemu EDR.
   1.2. Administracji Systemem EDR pozwalającą na samodzielne budowanie nowych polityk bezpieczeństwa, tworzenie własnych szablonów raportów, powiadomień/alarmów, przeszukiwania i grupowania zdarzeń, reguł korelacji, wyszukiwania i filtrowania, itd.

2. Warsztaty techniczne muszą rozpocząć się przed wdrożeniem Systemu EDR, nie wcześniej niż 15 Dni roboczych przed zaplanowaną datą wdrożenia.
3. Warsztaty muszą trwać min. 2 dni, w sumie nie mniej niż 12 godzin.
4. Warsztaty muszą być przeprowadzone w dwóch ustalonych przez strony terminach.
5. Warsztaty muszą być przeprowadzone w języku polskim. Cena oferowanych warsztatów musi obejmować pełne koszty ich przeprowadzenia, w szczególności koszty materiałów szkoleniowych, podróży, zakwaterowania, wyżywienia wykładowców. Warsztaty odbędą się w miejscu wskazanym przez Wykonawcę. Wymagana jest akceptacja miejsca przez Zamawiającego.
6. Wykonawca ma obowiązek zapewnić wykładowców posiadających odpowiednie kwalifikacje zawodowe i niezbędną wiedzę fachową w zakresie tematyki warsztatów potwierdzoną certyfikatem z oferowanej technologii wystawionym przez producenta wdrażanego rozwiązania.
7. Wykonawca dostarczy materiały warsztatowe uczestnikom warsztatów w formie elektronicznej w formacie ogólnie dostępnym umożliwiającym drukowanie oraz w formie papierowej na co najmniej 2 Dni robocze przed terminem rozpoczęcia warsztatów.
8. Wykonawca przygotuje i przekaże Administratorom Zamawiającego uczestniczącym w warsztatach imienne certyfikaty uczestnictwa.

V. Wymagania funkcjonalne dla Systemu EDR.

System EDR musi spełniać wszystkie wymagania funkcjonalne, o których mowa w załączniku nr B.

Część IV

I. Wymagania w zakresie wsparcia technicznego producenta dla Systemu NDR i Systemu EDR.

1. Serwis sprzętowy dla Systemu NDR świadczony będzie przez okres min. 12 miesięcy.
2. Wsparcie techniczne producenta dla Systemu NDR i Systemu EDR świadczone będą przez okres 12 miesięcy.
3. Bieg okresu serwisu sprzętowego oraz wsparcia technicznego producenta dla Systemu NDR i wsparcia technicznego dla Systemu EDR rozpoczyna się od dnia przekazania go do użytkowania, tj. po zakończeniu wdrożenia potwierdzonego Protokołem odbioru częściowego, oddzielnie dla każdego z systemów.
4. Wsparcie techniczne producenta powinno zawierać wsparcie świadczone telefonicznie i przy wykorzystaniu elektronicznego systemu obsługi zgłoszeń.

5. Wsparcie techniczne producenta musi być świadczone w trybie 24x7 (przez 24 godziny na dobę, 7 dni w tygodniu).
6. Usługa wsparcia technicznego producenta powinna obejmować dostęp do:
   5.1. Poprawek i nowych wersji wdrożonego Systemu NDR i Systemu EDR.
   5.2. Pomocy technicznej producenta.
   5.3. Aktualizacji informacji o zagrożeniach.
   5.4. Dokumentacji technicznej Systemu NDR i Systemu EDR.
   5.5. Konta w portalu producenta dla Zamawiającego umożliwiającego przeglądanie bazy wiedzy.
   5.6. Przewodników konfiguracyjnych i narzędzi diagnostycznych.
6. Zamawiający musi mieć możliwość zgłaszania zapytań o pomoc techniczną bezpośrednio do producenta Systemu NDR i Systemu EDR.
7. W okresie wsparcia technicznego Zamawiający musi mieć możliwość samodzielnego pobierania aktualizacji, poprawek i nowych wersji Systemu NDR i Systemu EDR.
8. Wykonawca przekaże Zamawiającemu informacje o gwarantowanym poziomie świadczenia usług serwisowych i wsparcia technicznego przez producenta dla oferowanych Systemów NDR i EDR.

II. Wymagania w zakresie Asysty technicznej świadczonej przez Wykonawcę dla Systemu NDR i Systemu EDR.

1. Usługa Asysty technicznej będzie świadczona przez ekspertów bezpieczeństwa Wykonawcy, którzy posiadają kwalifikacje zawodowe i doświadczenie niezbędne do wykonania zamówienia, posiadają certyfikat inżynierski wystawiony przez producenta oferowanego Systemu NDR, Systemu EDR oraz aktualny certyfikat inżynierski wystawiony przez producenta Palo Alto Networks Certified Network Security Engineer (PCNSE).
2. Pracownicy Wykonawcy świadczący usługę Asysty technicznej muszą posługiwać się w sposób komunikatywny językiem polskim.
3. Wykonawca jest zobowiązany w trakcie trwania Asysty technicznej do wykonywania gwarancyjnych usług serwisowych polegających w szczególności na diagnozowaniu i usuwaniu wszelkich Nieprawidłowości, a w razie konieczności do dostarczenia, wymiany i uruchomienia sprzętu zastępczego lub nowego, wolnego od wad, jak również do zapewnienia sprawnego działania oprogramowania Systemu NDR i Systemu EDR umożliwiającego jego wykorzystanie w zakresie funkcji opisanych w dokumentacji.
4. Usługa Asysty technicznej dla Systemu NDR i Systemu EDR musi być świadczona w okresie trwania wsparcia technicznego producenta, rozpoczynającym się w dniu pierwszego

protokolarnego odbioru wdrożenia jednego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego z wdrożenia), a kończącym się po 12 miesiącach od dnia protokolarnego odbioru wdrożenia kolejnego z ww. systemów (podpisania odpowiedniego Protokołu odbioru częściowego z wdrożenia).

5. Usługa Asysty technicznej powinna zawierać wsparcie świadczone telefonicznie i przy wykorzystaniu elektronicznego system obsługi zgłoszeń.
6. Asysta techniczna musi być świadczona min. we wszystkie dni tygodnia (m.in. w soboty i niedziele, włącznie z dniami ustawowo wolnymi od pracy) od godz. 8 do 22.
7. Poziom dostępności Systemu EDR i Systemu NDR w ciągu każdego miesiąca powinien wynosić nie mniej niż 99,6%. Dostępność oznacza czas bezawaryjnego działania Systemów w stosunku do całości czasu do którego odnosi się miara. Zamawiający wymaga, aby jednorazowy okres niedostępności nie przekroczył 90 min.
8. W ramach Asysty technicznej świadczonej dla Systemu NDR i Systemu EDR Wykonawca:
   8.1. Przejmuje na siebie wszelkie obowiązki związane z obsługą serwisową przedmiotu zamówienia.
   8.2. Zobowiązany jest świadczyć usługi utrzymania sprawności Systemu NDR i Systemu EDR w zakresie usunięcia Nieprawidłowości (Awaria krytyczna/Błąd/Usterka), z gwarantowanym czasem reakcji i naprawy opisanym w tabeli nr 1.
9. Usunięcie Nieprawidłowości w działaniu Systemu NDR i Systemu EDR musi być potwierdzone testem lub diagnostyką oraz dostarczonym raportem z przeprowadzonych prac.
10. Zweryfikowane i potwierdzone przez producenta awarie sprzętowe komponentów Systemu NDR usuwane będą maksymalnie w ciągu następnego Dnia roboczego, pod warunkiem że zgłoszenie o awarii zostało przekazane Wykonawcy do godz. 13. Awaria sprzętowa zgłoszona Wykonawcy po godz. 13 będzie usuwana najpóźniej w ciągu 2 Dni roboczych.
11. Do zapewnienia ciągłości pracy użytkowników Systemu NDR dopuszcza się możliwość wprowadzenia obejść zastępczych w celu usuwania Awarii krytycznej.
12. Usługa Asysty technicznej wykonywana będą poprzez dostęp zdalny lub w razie konieczności w miejscu zainstalowania Systemu NDR i Systemu EDR.
13. Rodzaj Nieprawidłowości określa Zamawiający na podstawie opisu Nieprawidłowości.
14. Wykonawca jest zobowiązany do prowadzenia rejestru świadczenia usługi Asysty technicznej i podawania danych dotyczących (raportowania) świadczenia usługi Asysty technicznej w terminie 5 Dni roboczych od daty zakończenia każdego miesięcznego okresu świadczenia usługi. Raport musi zawierać zestawienie wszystkich zgłoszeń w danym miesiącu, ze wskazaniem dat i godzin

zgłoszeń, potwierdzenia przyjęcia zgłoszenia i udzielenia odpowiedzi.

Tabela nr 1 – Czas usuwania Nieprawidłowości.

Lp.	Rodzaj Nieprawidłowości	Opis Nieprawidłowości	Czas Reakcji	Czas Naprawy
1	Awaria krytyczna	Całkowite unieruchomienie Systemu NDR lub Systemu EDR uniemożliwiające korzystanie oraz uniemożliwiająca realizację ochrony przed atakami. Brak możliwości zastosowania rozwiązania obejściowego	do 2 godzin od zgłoszenia przez Zamawiającego	do 8 godzin od czasu reakcji jeśli awaria nie dotyczy warstwy sprzętowej
				do 1 Dnia roboczego od czasu reakcji jeśli awaria dotyczy warstwy sprzętowej i zgłoszona została do godz. 13
				do 2 Dni roboczych od czasu reakcji jeśli awaria dotyczy warstwy sprzętowej i zgłoszona została po godz. 13
2	Błąd	Znaczny spadek wydajności Systemu NDR lub Systemy EDR. Niedostępne są wybrane funkcjonalności Systemu NDR/EDR istotne dla Zamawiającego pozwalające jednak na dalszą realizację ochrony przed atakami. Możliwość zastosowania rozwiązania obejściowego	do 4 godzin od zgłoszenia przez Zamawiającego	do 2 Dni Roboczych - zastosowanie rozwiązania obejściowego od czasu reakcji
3	Usterka	Niedostępne są niektóre funkcjonalności Systemu NDR lub Systemu EDR mało istotne dla Zamawiającego.	do 24 godzin od zgłoszenia przez Zamawiającego	do 5 Dni Roboczych od czasu reakcji

III. Wymagania w zakresie Godzin eksperckich świadczonych przez Wykonawcę dla Systemu NDR i Systemu EDR.

1. Usługa Godzin eksperckich będzie świadczona przez zespół ekspertów bezpieczeństwa, którzy posiadają kwalifikacje zawodowe i doświadczenie niezbędne do wykonania zamówienia, posiadają certyfikat inżynierski wystawiony przez producenta oferowanego Systemu NDR, Systemu EDR oraz aktualny certyfikat inżynierski wystawiony przez producenta Palo Alto Networks Certified Network Security Engineer (PCNSE).
2. Pracownicy Wykonawcy świadczący usługę Godzin eksperckich muszą posługiwać się w sposób komunikatywny językiem polskim.

3. Usługa Godzin eksperckich dla Systemu NDR i Systemu EDR musi być świadczona w okresie trwania wsparcia technicznego producenta.
4. Usługi świadczone w ramach Godzin eksperckich muszą być realizowane min. w Dni robocze od godz. 8 do 18.
5. W ramach świadczonych Godzin eksperckich dla Systemu NDR i Systemu EDR Wykonawca zobowiązany będzie do:
   5.1. Rozwiązywania bieżących problemów i zagadnień dotyczących funkcjonowania, które wymagają dokonywania zmian konfiguracyjnych we wdrożonych systemach.
   5.2. Wdrażania poprawek i aktualizacji systemów.
   5.3. Konsultacji i wsparcia dotyczącego utrzymania eksploatowanego systemu, dokonywania zmian w optymalizacji reguł i polityk bezpieczeństwa.
   5.4. Konsultacji i wsparcia w analizie zdarzeń bezpieczeństwa zarejestrowanych przez System NDR i System EDR.
6. Usługa Godzin eksperckich będzie świadczona w wymiarze wynoszącym do 200 Roboczogodzin w całym okresie korzystania przez Zamawiającego z usługi.
7. Usługa Godzin eksperckich wykonywana będzie poprzez dostęp zdalny lub w razie konieczności w miejscu zainstalowania Systemu NDR i Systemu EDR (w zależności od potrzeb Zamawiającego).
8. Zamawiający, w przypadku pojawiających się potrzeb, związanych z kwestiami opisanymi w pkt 5, każdorazowo zgłosi potrzebę skorzystania z usługi Godzin eksperckich poprzez przekazanie drogą elektroniczną Zlecenia.
9. Zlecenia muszą być rejestrowane w systemie zgłoszeń serwisowych Wykonawcy, a Zamawiający musi mieć możliwość monitorowania przyjętych i obsłużonych Zleceń (datę i czas rejestracji, reakcji, naprawy, treść Zlecenia, jego status, informację o osobie obsługującej i zgłaszającej Zlecenie) w systemie Wykonawcy.
10. Wykonawca ma obowiązek niezwłocznie potwierdzić Zamawiającemu przyjęcie Zlecenia, każdorazowo nie później niż następnego Dnia roboczego po dniu otrzymania Zlecenia. Termin rozpoczęcia realizacji Zlecenia nie może być dłuższy niż 1 Dzień roboczy licząc od dnia potwierdzenia przez Wykonawcę przyjęcia Zlecenia do realizacji.
11. Po wykonanym Zleceniu, Wykonawca sporządzi i przekaże Zamawiającemu w formie przynajmniej dokumentowej, dokumentację obejmującą zakres wykonanych czynności w ramach Godzin eksperckich, zawierającą co najmniej:
    1) wykaz zrealizowanych czynności wraz ze wskazaniem liczby Roboczogodzin;
    2) raport potwierdzający prawidłowe wykonanie Zlecenie.

12. Potwierdzeniem prawidłowego wykonania usługi Godzin eksperckich będzie podpisany przez Strony bez zastrzeżeń Protokół odbioru Zlecenia.
13. Rozliczenie z tytułu świadczenia usługi Godzin eksperckich będzie odbywało się po zakończeniu kwartału kalendarzowego.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

Załącznik nr A

1. Wymagania funkcjonalne dla Systemu NDR.

Pola w kolumnie „Opis spełnienia wymagań" wypełnia Wykonawca. Zamawiający oczekuje wskazania do odniesienia w specyfikacji producenta opublikowanej na stronie producenta lub załączonej do oferty specyfikacji producenta potwierdzającej spełnienie wymagań.

Lp.	Wymagania funkcjonalne dla Systemu NDR	Opis spełnienia wymagań
A	**Analiza ruchu sieciowego**	
A-1	Sondy przeznaczone do inspekcji ruchu sieciowego muszą posiadać wbudowane funkcjonalności analizy protokołów komunikacyjnych. Wymagana jest obsługa co najmniej następujących protokołów, aplikacji i systemów pozwalających na wymianę informacji: SIP, SMB, Exchange, Sharepoint, DNS, HTTP, FTP, SMTP, POP3, IMAP4, Oracle, DB2, Telnet	
A-2	System musi być w stanie wykryć wystąpienie danych przesyłanych przy wykorzystaniu minimum następujących protokołów, aplikacji i systemów pozwalających na wymianę informacji, co najmniej na styku z siecią Internet: 1) SMTP, POP3, IMAP4, FTP, HTTP, HTTPS, Telnet, LDAP, Bittorrent, RDP, RTSP, SSL, TLS, X11; 2) Googlemail, Squirrelmail, Yahoomail; 3) Facebook, Linkedin, Twitter; 4) IRC, Jabber/XMPP, Kazaa, Gnutella; 5) SMB, DB2, MSSQL, Oracle, Exchange/Kerberos	
A-3	Rejestrowane metadane muszą zawierać informacje o parametrach analizowanej sesji, takie jak: adresy i porty komunikacyjne, pola nagłówków mime, multipart, informacje o protokołach komunikacji i aplikacjach, informacje o atrybutach aplikacji i protokołów, w tym protokołów szyfrowanych, informacje o zawartości komunikacji, w szczególności: 1) Client IP 2) Client Country 3) Client Port 4) Server IP 5) Server Country 6) Server Port 7) Timestamp 8) Protocol 9) Transport 10) Filename 11) Filesize 12) Filetype 13) User 14) From 15) To 16) Subject 17) Host 18) URL 19) Referer 20) Location 21) Proxy 22) Proxy-Connection 23) Proxy port 24) UserAgent 25) Server 26) Via 27) X-Forwarder-F 28) StatusCode 29) CalllD 30) Client 31) Command 32) Connection	

	33) Database 34) DirectoryDN 35) Domain 36) Encrypted 37) Hash 38) IssuerName 39) KeyLenght 40) KeyUsage 41) SubjectName 42) StartDate 43) EndDate 44) Mode 45) Share 46) SQL 47) Version	
A-4	System musi zapewniać wykrywanie przypadków enkapsulacji lub tunelowania ruchu sieciowego (co najmniej za pomocą protokołów: ICMP, DNS, HTTP/HTTPS, SSH, TLS) na standardowych i niestandardowych dla w/w protokołów portach.	
A-5	System musi zapewniać wykrywanie przypadków omijania autoryzowanych serwerów Proxy	
A-6	System musi zapewniać wykrywanie przypadków wykorzystywania zewnętrznych, nieautoryzowanych serwerów Proxy.	
A-7	System musi zapewniać wykrywanie słabych mechanizmów uwierzytelniania lub szyfrowania.	
A-8	System musi zapewniać wykrywanie komunikacji z niepożądanymi hostami/sieciami (np. powszechnie znane serwery C&C, TOR, skompromitowane serwery web, serwery powiązane z ransomware itp. oraz samodzielnie budowane i aktualizowana własna lista sieci / serwerów / nazw domenowych / adresów URL).	
A-9	System musi zapewniać wykrywanie przypadków przesyłania informacji jawnym tekstem w protokołach, w których oczekiwane jest jej szyfrowanie i odwrotnie - przesyłanie informacji w formie zaszyfrowanej w protokołach, w których oczekiwane jest przesyłanie jej jawnym tekstem.	
A-10	System musi zapewniać wykrywanie nietypowych zapytań DNS, np. świadczących o eksfiltracji danych lub zainstalowaniu niepożądanego oprogramowania.	
A-11	System musi zapewniać inspekcję transmisji DNS (również na portach innych niż 53), przynajmniej w oparciu o weryfikację: 1) Długości nazw domen; 2) Poprawnej długości pakietu - z parametryzowaniem tej wartości osobno dla TCP i UDP; 3) Poprawności parsowania pakietu; 4) Dozwolonych Resource Records (RR); 5) Poprawności długości RR; 6) List reputacyjnych (blacklists) - dostarczanych przez producenta, z możliwością skonfigurowania własnych źródeł reputacji.	
A-12	System musi zapewnić możliwość konfiguracji białych list (wyjątków) dla inspekcji DNS. System musi oferować wsparcie dla wskazywania źródeł i automatycznego pobierania list wyjątków - dla nazw domen oraz adresów IP, bez konieczności ręcznej aktualizacji listy wyjątków.	
B	**Wykrywanie i przeciwdziałanie propagacji złośliwego oprogramowania**	
B-1	System musi w czasie rzeczywistym analizować ruch sieciowy na wszystkich 65 535 portach TCP i UDP oraz niezależnie od portu wykrywać i analizować zawartość komunikacji sieciowej	
B-2	System musi poprawnie wykrywać protokoły i aplikacje nawet jeśli przesyłane są na niestandardowych portach	
B-3	System musi wykrywać w ruchu sieciowym i dekodować aplikacje oraz przesyłane za ich pomocą treści; inspekcja musi opierać się na analizie całych sesji oraz poszczególnych pakietów	

B-4	Sondy analizujące ruch sieciowy na wszystkich portach TCP/UDP, niezależnie od trybu pracy (in-line, out-of-band), muszą pozwalać na zapisywanie przesyłanych danych w oryginalnej postaci (packet capture) i dołączanie ich do alertu przekazywanego do urządzenia zarządzającego.	
B-5	System musi rozpoznawać i pozwalać na analizę minimum następujących formatów plików i systemów kodowania: 1) Base64 2) bzip2 3) Deflate 4) Gzip 5) Html 6) Mail 7) Message 8) Mime 9) ms-access-mdb 10) ms-excel 11) ms-office 12) ms-powerpoint 13) ms-rtf 14) ms-word 15) ms-visio 16) Multipart 17) Pdf 18) PGP 19) Postscript 20) quoted-printable 21) Rar 22) rfc822 23) Soap 24) Tar 25) Text 26) Urlencode 27) Uuencode 28) Xml 29) Ymsg 30) Zip 31) 7zip	
B-6	System musi wspierać procesowanie ruchu szyfrowanego Google (QUIC).	
B-7	System musi pozwalać na rekursywne dekodowanie protokołów i rekursywna analizę plików w obrębie sesji sieciowych w celu wykrywania przypadków występowania w nich kodu złośliwego. Przykładowe działanie rekursywnej analizy: odnalezienie w sesji TCP protokołu POP3 zabezpieczonego przy użyciu TLS na niestandardowym porcie komunikacyjnym, odnalezienie w protokole POP3 wiadomości e-mail z załącznikiem ZIP, odnalezienie w pliku ZIP dokumentu DOC, ustalenie, ze odnaleziony dokument jest w istocie dokumentem PDF ze zmienionym rozszerzeniem, odnalezienie w dokumencie PDF zagnieżdżonego kodu złośliwego JavaScript w oparciu o analizę statyczną kodu.	
B-8	System musi pozwalać na wyświetlenie wyników każdego etapu rekursywnej analizy protokołów, rekursywnej analizy plików i zdekodowanej zawartości. Ponadto, w przypadku wygenerowania alertu System musi zapisywać zdekodowane pliki wraz z całą ich zawartością na każdym etapie dekodowania (dane śledcze) oraz umożliwiać w oknie widoku alertu wizualizację nagłówków protokołów klienta i serwera w transmisji sieciowej.	
B-9	System musi zapewniać wykrywanie i ochronę przed złośliwym kodem i zagrożeniami typu APT za pomocą następujących mechanizmów: 1) Reputacja źródła oraz celu transmisji danych (serwery Command and Control - C&C, phishing, malware) 2) Sygnatury złośliwego kodu dostarczonej przez producenta	

	3) Gotowe zestawy polityk definiujące charakterystyki zagrożeń 4) Emulacja w celu deobfuskacji (dekompresji, deszyfrowania) złośliwego kodu. 5) Statyczna analiza kodu w celu wykrywania cech charakterystycznych złośliwego kodu 6) Uruchomienie złośliwego kodu w środowisku wirtualnym w celu uzyskania informacji o funkcjonalności złośliwego kodu 7) Wykrywanie komunikacji C&C poprzez analizę protokołów i aplikacji sieciowych (m.in. tunelowanie, niestandardowe parametry protokołów i aplikacji, odwołania do „sinkholes", wykrywanie „reverse shell") oraz powiązanie przesłania podejrzanych obiektów do stacji roboczej z następującą po nim nietypową aktywnością sieciową z badanej stacji (m.in. tunelowanie, nawiązanie komunikacji IRC, wykrycie protokołów administracyjnych, przesłanie treści do pastebin.com, generowanie komunikacji HTTP z niestandardowymi parametrami pola User-Agent). 8) Wykrywanie ataków na serwery usług, m.in. poprzez wykorzystanie podatności implementacji protokołów TLS, SMB (w tym Heartbleed, EternalBlue i inne). 9) Automatyczne, cykliczne przeszukanie wszystkich danych zgromadzonych w urządzaniu pamięci sieciowej ze względu na nowo zaktualizowane przez System sygnatury zagrożeń nie rzadziej niż raz dziennie. Przykładowo: przeszukanie całości danych na urządzeniach pamięci sieciowej i wygenerowanie alertu o odnalezieniu złośliwego pliku Javascript zagnieżdżonego w plikach PDF przesyłanych w kanale poczty firmowej i przy użyciu protokołu IMAP podczas pobierania poczty z zewnętrznych serwisów przez pracowników. 10) Wykrywanie technik i taktyk prowadzenia ataków przez ciągłe przeszukiwanie gromadzonych danych w urządzeniu pamięci sieciowej pod kątem spełnienia reguł korelacyjnych wykrywających m.in. rozłożone w czasie, wieloetapowe procesy przejmowania stacji roboczej z wykorzystaniem różnych kanałów komunikacji w różnych etapach ataku oraz identyfikację powolnych wycieków danych.	
B-10	System musi automatycznie analizować wykryty kod złośliwy poprzez automatyczne uruchomienie złośliwego kodu w wyizolowanym środowisku wirtualnym (piaskownicy, zainstalowanej on-site) w celu analizy zagrożenia i jego potencjalnych skutków. W wyniku automatycznej analizy System musi tworzyć sygnatury wykrytych zagrożeń oraz dostarczać szczegółowych informacji o skutkach działania złośliwego kodu w systemie docelowym (np. instalowane pliki, modyfikacje plików, modyfikacje wpisów w rejestrze).	
B-11	W wyniku automatycznej analizy System musi dostarczać szczegółowych informacji o skutkach działania złośliwego kodu w systemie operacyjnym (uruchamiane procesy, tworzone lub modyfikowane pliki, modyfikacje wpisów w rejestrze, generowany ruch sieciowy) i ocenić jego szkodliwość.	
B-12	System musi wspierać wszystkie popularne formaty, w tym m. in: exe, html, java-class, ms-excel, ms-office, ms-powerpoint, ms-rtf, ms-word, pdf, zip.	
B-13	Detonacja próbek w piaskownicy musi być dokonywana w systemie MS Windows min. wersji 10 Professional, 64-bit.	
B-14	System musi być wyskalowany do analizy min. 8 000 próbek w ciągu 24 godz.	
B-15	System musi oferować możliwość konfiguracji opcji automatycznego przesyłania podejrzanych próbek: wszystkich obsługiwanych typów plików, wybranych typów plików, żadnego z obsługiwanych typów plików.	
B-16	System musi udostępniać możliwość ręcznego wysyłania plików z panelu Systemu zarządzającego do analizy i prezentowanie wyników analizy w taki sam sposób jak plików wysyłanych automatycznie.	

B-17	System powinien posiadać predefiniowane polityki bezpieczeństwa oraz słowniki słów kluczowych i fraz, przynajmniej w języku angielskim.	
B-18	System musi umożliwiać wykrywanie i blokowanie złośliwego kodu na podstawie stale aktualizowanych sygnatur dostarczanych przez producenta.	
B-19	System musi pozwalać na tworzenie polityki bezpieczeństwa wykrywających następujące typy danych: 1) Rozpoznawane formaty plików; 2) Pliki zaszyfrowane; 3) Sygnatury binarne plików zarejestrowanych w systemie; 4) Słowa kluczowe lub ich synonimy; 5) Sekwencje słów kluczowych lub frazy; 6) Wyrażenia regularne.	
B-20	Polityki Systemu muszą umożliwiać dla każdej sesji sieciowej określenie następujących warunków: 1) W zawartości komunikacji System musi umożliwiać weryfikację dekodowanej treści pod kątem jej zawartości za pomocą następujących mechanizmów: 1.1) Suma kontrolna md5 i sha256 pliku lub jego elementów składowych; 1.2) Poszukiwania wystąpień słów i fraz z możliwością określenia wagi każdego z wystąpień, rozpoznawania bądź ignorowania wielkości znaków oraz kresu górnego ilości zliczanych wystąpień słów i fraz dla każdej definicji z osobna; 1.3) Poszukiwania wystąpień sekwencji słów kluczowych i fraz w określonej kolejności z możliwością występowania dowolnego tekstu pomiędzy zdefiniowanymi słowami kluczowymi, frazami; 1.4) Poszukiwania fraz językowych bądź pojedynczych słów z wykorzystaniem pełnego silnika wyrażeń regularnych zgodnego z Perl Compatible Regular Expression (PCRE); 1.5) Mechanizmu kwalifikującego dane za pomocą profilowania identyfikatorów, który w szczególności będzie obsługiwał polskie formaty PESEL, REGON, NIP z weryfikacją poprawności oraz numery kart kredytowych, IBAN, SWIFT; 1.6) Mechanizmu wykrywania plików zaszyfrowanych, przynajmniej: Microsoft Excel, Microsoft Word, chronionych PDF, szyfrowania PGP, 7Zip, ZIP, RAR; 1.7) Rejestracji obrazów (pliki graficzne) i wykrywania ich w ruchu sieciowym, także w sytuacji kiedy zostaną osadzone w dokumencie; 1.8) Wyszukiwania w treści transmisji i treści przesyłanych dokumentów zdefiniowanych adresów URL pozyskiwanych i odświeżanych automatycznie ze wskazanych źródeł (wymagana możliwość dodawania własnych źródeł list URL); 1.9) Wsparcie dla przeszukiwania treści przy użyciu reguł YARA. 2) W zakresie określania lokalizacji System musi umożliwiać utworzenie warunków w oparciu o źródłowy/docelowy adres IP, zakres adresów lub sieć, reputacja źródłowego/docelowego adresu IP/domeny (phishing, malware) w oparciu o stale aktualizowane źródła reputacji z możliwością konfiguracji automatycznie aktualizowanych w Systemie własnych źródeł reputacji, lokalizacja geograficzna źródłowego/docelowego adresu IP; 3) W zakresie parametrów kanału komunikacji: atrybuty aplikacji/protokołu (niezależnie od portu), parametry specyficzne dla aplikacji/protokołu (nazwa użytkownika, adres e-mail, temat wiadomości, adres URL, treść zapytania SQL, nazwa pliku, czas trwania sesji, rozmiar przesyłanych danych, rodzaj szyfrowania, siła szyfru i inne), typy plików i specyficzne dla nich atrybuty (np.: typ pliku niezależnie od jego rozszerzenia, autor dokumentu, zawartość stopki, czas utworzenia, czas modyfikacji, wskazanie	

	zagnieżdżenia obiektu w ścieżce dekodowania), zastosowane kodowanie plików (np.: rodzaj kompresji), docelowy/źródłowy port TCP, długość trwania i rozmiar sesji, dzień tygodnia i godzina, sygnatury aplikacji i protokołów.	
B-21	System musi umożliwiać dowolne łączenie wielu definicji lokalizacji, kanału komunikacji i zawartości w jednej polityce z zastosowaniem wyrażeń logicznych. System musi umożliwiać łączenie polityk w zestawy oraz umożliwiać wykorzystanie tych samych wyrażeń i reguł w wielu politykach jednocześnie z możliwością przypisania tych samych polityk do różnych zestawów i przydzielanie zestawów do dowolnej ilości sond, w tym sond różnych typów.	
B-22	Analiza ruchu sieciowego w oparciu o polityki musi odbywać się w czasie rzeczywistym.	
B-23	Mechanizmy weryfikacji dekodowanej treści muszą umożliwiać powiadamianie o zagrożeniach oraz blokowanie niebezpiecznych sesji w czasie rzeczywistym w zależności od konfiguracji polityk.	
B-24	System musi umożliwiać podejmowanie akcji w zależności od wartości dowolnego z wymienionych parametrów lub ich zestawu. Lista dostępnych akcji dla stworzonej polityki musi umożliwiać: wygenerowanie alarmu, zarejestrowanie szczegółowego logu zdarzenia, zarejestrowanie zapisu przesyłanych danych naruszających uruchomione polityki, zablokowanie ruchu, przepuszczenie ruchu, usunięcie załączników wiadomości email i przesłanie samej treści wiadomości, przeniesienie wiadomości do kwarantanny, oznaczenie sesji/plików/dokumentów i ich elementów składowych w zależności od zawartości bez konieczności zapisu treści zdarzenia i generowania alertu.	
B-25	Sondy analizujące ruch na wszystkich portach TCP/UDP muszą mieć możliwość działania w trybie out-of-band - poprzez prowadzenie nasłuchu na porcie typu SPAN. Sondy działające w tym trybie musza pozwalać na wymuszenie zerwania niepożądanych sesji poprzez wykorzystanie pakietów TCP Reset.	
B-26	Sondy analizujące ruch na wszystkich portach TCP/UDP muszą mieć możliwość działania w trybie in-line poprzez analizę przesyłanego przez urządzenie ruchu. Sondy działające w tym trybie muszą pozwalać na odrzucanie pakietów niepożądanych sesji.	
C	**Ochrona poczty elektronicznej**	
C-1	System musi umożliwiać tworzenie własnych polityk opartych o wartości parametrów komunikacji sieciowej TCP/IP, wartości parametrów komunikacji SMTP, wartości parametrów nagłówków wiadomości e-mail, wartości parametrów opisujących metadane załączników (typ, rozmiar, wielkość itp.).	
C-2	System musi mieć mechanizm analizy ruchu pocztowego w celu wykrywania, powstrzymywania i rejestrowania: 1) Wiadomości zawierających złośliwą zawartość z wykorzystaniem mechanizmów: rekursywnego dekodowania/wyodrębniania zawartości, deobfuskacji zawartości (automatyczne wykrywanie zagnieżdżenia, zaciemnienia, kodowania zawartości), analizy na podstawie sygnatur, emulacji kodu, uruchomienia kodu w kontrolowanych warunkach i analizy jego zachowania (Sandboxing), informacji o znanych źródłach zagrożeń w sieci (adresy IP, URL), analizy behawioralnej, polityk opisujących charakterystyczne cechy zagrożeń (na podstawie właściwości wiadomości i zawartości); 2) Wiadomości zawierających dane poufne na podstawie zdefiniowanych polityk zawierających: definicje słów kluczowych, sekwencji słów kluczowych oraz słowników słów kluczowych z uwzględnieniem punktacji (wag) i powtarzalności, definicje zawartości opisanej za pomocą wyrażeń regularnych, sygnatury plików, sygnatury częściowych zawartości, metadane zawartości (nazwa, typ, data utworzenia, rozmiar pliku), predefiniowane wzorce danych takich jak PESEL, REGON, NIP z możliwością dostosowania czułości systemu.	

C-3	Sondy pocztowe muszą posiadać możliwość pracy w trybie działania Mail Transport Agent (MTA) i brać aktywny udział w transmisji SMTP.	
C-4	Sonda poczty musi posiadać możliwość obsługi kwarantanny dla poczty przychodzącej i wychodzącej - przez administratora Systemu przy użyciu panelu urządzenia zarządzającego, jak również (dla zdefiniowanych przez administratora przypadków naruszeń) poprzez pracowników za pomocą generowanych przez system powiadomień przy użyciu kanału pocztowego i interpretacji odpowiedzi udzielonych przez pracowników	
C-5	System musi umożliwiać długoterminowe rejestrowanie metadanych historycznych wszystkich wiadomości e-mail w ruchu SMTP w sposób umożliwiający ich przeszukiwanie na podstawie metadanych komunikacji sieciowej TCP/IP (adresy, porty), metadanych protokołu SMTP (serwery pocztowe, nadawca/adresat, temat, rozmiar, kodowanie, nagłówki wiadomości) oraz metadanych zawartości (typ/nazwa/rozmiar/suma kontrolna pliku).	
C-6	System musi umożliwiać automatyczne wyszukiwanie wystąpienia nowo odkrytych zagrożeń w danych historycznych.	
C-7	System musi umożliwiać automatyczne przeszukiwanie danych historycznych ze względu na sekwencję oraz częstotliwość wystąpień.	
C-8	System musi umożliwiać analizę wiadomości pocztowych z wykorzystaniem mechanizmu dostarczanych przez producenta polityk opartych o wartości parametrów komunikacji sieciowej TCP/IP, wartości parametrów komunikacji SMTP, wartości parametrów nagłówków wiadomości e-mail, wartości parametrów opisujących metadane załączników (typ, rozmiar, wielkość, autor plików itp.).	
C-9	System musi umożliwiać rejestrowanie, odrzucanie, kwarantannę oraz przekierowanie wiadomości pocztowych na bazie polityk.	
D	**Zarządzanie systemem**	
D-1	Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu jak również pomiędzy poszczególnymi jego komponentami musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.	
D-2	System musi posiadać udokumentowane API umożliwiające integrację z innymi systemami wspierającymi zarządzanie środowiskiem IT, dostępne poprzez centralny system zarządzania. Opcje osiągalne z poziomu API muszą oferować przynajmniej: wyszukiwanie i filtrowanie alarmów, możliwość pobierania zapisów plików stanowiących naruszenie wykryte przez System.	
D-3	System musi pozwalać na zarządzanie wszystkimi komponentami dokonującymi analizy treści i gromadzenia danych oraz wszystkimi ich parametrami takimi, jak: konfiguracja trybów pracy, tworzenie polityk analizy, konfigurację zasad alarmowania, retencji danych, zasad eksportu danych do innych systemów bezpieczeństwa, zasad wykonywania kopii bezpieczeństwa, propagowanie poprawek i aktualizacje oprogramowania, zarzadzanie licencjami przy pomocy komponentu realizującego funkcję centralnego systemu zarządzania.	
D-4	System musi umożliwiać zarządzanie poprzez dedykowane GUI, CLI, API oraz język skryptowy.	
D-5	Moduł zarządzania musi wspierać następujące metody uwierzytelniania: LDAP, TACACS, RADIUS, AD.	
D-6	Moduł zarządzania musi udostępniać interfejs WEB, który wspiera wszystkie funkcje konfiguracji, zarządzania politykami, analizy danych oraz raportowanie	
D-7	Muszą być wspierane przeglądarki internetowe w najnowszych wersjach: 1) Mozilla Firefox; 2) Google Chrome; 3) Edge.	
D-8	Moduł zarządzania musi wspierać zarządzanie z wykorzystaniem ról (RBA).	
D-9	Zarządzanie z wykorzystaniem ról (RBA) musi umożliwiać grupowanie ról.	

D-10	Zarządzanie z wykorzystaniem ról (RBA) musi umożliwiać ograniczenie dostępu administratorów do funkcji konfiguracyjnych.	
D-11	System musi umożliwiać dostarczanie alertów do wybranych grup RBA.	
D-12	Interfejs użytkownika systemu zarządzania musi być dostosowany do ról użytkowników. Opcje niedostępne dla danej roli nie mogą być widoczne w interfejsie.	
D-12	Moduł zarządzania musi umożliwiać ograniczenie do danych analitycznych ze względu na role.	
D-13	Centralny system zarządzania musi pozwalać na tworzenie kont użytkowników Systemu o różnych poziomach uprawnień. Wymagane jest aby oferowane rozwiązanie pozwalało na granularne zarządzanie uprawnieniami użytkowników poprzez łączenie użytkowników w grupy, definiowanie uprawnień dostępu do odczytu i zapisu oraz braku dostępu dla kluczowych obszarów zarzadzania Systemem takich jak: alerty, szczegóły alertów, kwarantanna, raporty, polityki, użytkownicy, administratorzy komponentów, administrator komponentu zarzadzania, audytor, pamięć sieciowa. W obszarze uwierzytelniania użytkowników Systemu wymagana jest możliwość integracji z LDAP/AD w celu identyfikacji użytkownika przesyłającego określone dane . Wymagane jest dostarczenie systemu dla nielimitowanej liczby użytkowników	
D-14	W ramach urządzenia zarządzającego, dla wszystkich obsługiwanych przez nie komponentów, musi być dostępna funkcjonalność wewnętrznego audytu, umożliwiająca logowanie wszystkich działań podjętych przez administratorów Systemu takich jak: logowanie do Systemu, zmiana konfiguracji, modyfikacja polityk, zestawów polityk, zarzadzania alertami, dostęp do alertu, pobranie danych śledczych powiązanych z alertem, usuwania alertu, dostęp do raportów i ich modyfikacja, dostęp do pamięci sieciowej. System musi zapewniać ciągły eksport logu audytu przynajmniej przy użyciu protokołu syslog.	
D-15	System musi zapewniać zintegrowany system obsługi zdarzeń - otwieranie zgłoszeń, przypisywanie zdarzeń do użytkowników Systemu, obsługę (przydzielanie zdarzeń do operatorów w Systemie), zamykanie zdarzeń w panelu z nadaniem statusu zamknięcia. Musi istnieć możliwość filtrowania i wyszukiwania zdarzeń w panelu w oparciu o status przypisanych zdarzeń i użytkowników, do których zdarzenia są przypisane.	
D-16	System musi oferować możliwość konfigurowania polityk retencji zdarzeń (alertów) w oparciu o kryteria: priorytet alertu, sonda z jakiej napłynął alert, polityka która wyzwoliła alert, użytkownik do którego przypisane są alerty, grupa do której przypisany jest alert. Musi istnieć możliwość tworzenia dowolnej ilości polityk retencji zdarzeń w oparciu o wyżej zdefiniowane kryteria z możliwością łączenia parametrów różnych kryteriów. Przed usunięciem alertów spełniających zdefiniowane w politykach retencji warunki System musi oferować przesłanie ich do zewnętrznego zasobu sieciowego przy użyciu przynajmniej protokołów FTP i SFTP.	
D-17	Urządzenie zarządzające musi posiadać funkcję raportowania o ciągłości pracy sond i urządzenia pamięci sieciowej oraz raportować wszelkie odchylenia. W przypadku wykrycia odchyleń wymaga się aby System prezentował informacje w panelu systemu zarządzania oraz miał opcję wysyłania powiadomień e-mail.	
D-18	Wymaga się aby System umożliwiał importowanie informacji o zagrożeniach z zewnętrznych źródeł, przynajmniej w oparciu o: Adres IP, nazwę domeny, URL, sumy kontrolne MD5 i SHA256. Wspierane formaty dostarczania informacji o zagrożeniach to przynajmniej: STIX, TAXII, CSV. Import i propagacja odświeżonych informacji o zagrożeniach do sond musi odbywać się w sposób automatyczny.	
D-19	System musi umożliwiać przeszukiwanie całości zapisanych informacji o analizowanym ruchu (również informacji o ruchu, który nie narusza ustalonych polityk) przesyłanych z sond za pomocą interfejsu graficznego dostępnego w ramach centralnego systemu zarządzania. System musi zapewniać możliwość analizy poprzez wizualizację zarejestrowanej	

	reprezentacji całości ruchu sieciowego oraz reprezentacji przesyłanej treści sesji sieciowych powiązanych z alertami zgłoszonymi w wyniku naruszenia polityk tak, aby możliwe było rozpoznanie kontekstu zaistniałego naruszenia.	
D-20	Przeszukiwanie całości zapisanych informacji o analizowanym ruchu musi być prezentowane w sposób umożliwiający interaktywne przeglądanie graficznej reprezentacji ruchu sieciowego i przesyłanej treści, spełniających warunki zawarte w zapytaniu oraz pozwalać na wykonywania dalszych zapytań inicjowanych za pomocą menu kontekstowego dostępnego w obrębie panelu obrazującego wyniki lub alternatywnie poprzez doprecyzowanie zapytania w widoku zaawansowanym	
D-21	Interfejs musi mieć zapewnione zaawansowane wyszukiwanie pozwalające definiować kryteria wyszukiwania przynajmniej w oparciu o adres IP, port, protokół transmisji, zdekodowane atrybuty kanału komunikacji oraz zdekodowane informacje opisujące treść, sondę na której wystąpiło zdarzenie. Musi być też zapewniona możliwość budowania złożonych filtrów przynajmniej w oparciu o operatory logiczne AND i OR pomiędzy zdefiniowanymi warunkami, z możliwością zagnieżdżania warunków, stosowania wykluczeń, podawania list możliwych wartości w jednym polu, wykorzystywania relacji zawierania treści oraz sprawdzania czy badany parametr transmisji ma przypisaną jakąkolwiek wartość.	
D-22	Zamawiający wymaga, aby oferowane rozwiązanie wyposażone było w mechanizmy wykrywania i korelacji zdarzeń sieciowych rozciągniętych w czasie w celu wykrywania tzw. „powolnych wycieków" danych.	
D-23	W Systemie musi istnieć możliwość automatycznego, cyklicznego przeszukiwania zgromadzonych w urządzeniu pamięci sieciowej (magazynie sieciowym) informacji opisujących każdą sesję sieciową, transmisje, przesyłane pliki i ich elementy składowe (niezależnie od poziomu zagnieżdżenia treści) w oparciu o reguły dostarczane przez producenta, jak również tworzone indywidualnie przez Zamawiającego - reguły takie muszą pozwalać na korelację odległych od siebie informacji, sprawdzając je w oparciu o dostarczony opis kolejnych zestawów warunków z określeniem czasu pomiędzy kolejnymi krokami opisującymi naruszenie oraz czasu pomiędzy pierwszym a ostatnim krokiem naruszenia. System musi pozwalać na opisanie przynajmniej 5 kroków przy użyciu zestawu warunków połączonych operatorami logicznymi.	
D-24	System musi posiadać możliwość szybkiego przeszukania danych w magazynie sieciowym (wystąpienia sesji sieciowych) bez konieczności stosowania mechanizmów optymalizacji zapytań w zależności od typu przeszukiwanych danych.	
D-25	System musi umożliwiać przeszukiwanie danych urządzenia pamięci sieciowej (magazynu sieciowego) według czasu ich wystąpienia wśród wszystkich zarejestrowanych sesji niezależnie od protokołu i kierunku transmisji.	
D-26	System musi pozwalać na definiowanie powiadomień, przesyłanych z chwilą odnotowania alertu, pozwalających na minimum wysłanie wiadomości e-mail do administratora w przypadku naruszenia zdefiniowanych polityk oraz w przypadku wykrycia niepożądanego ruchu.	
D-27	System musi posiadać możliwość ustalania warunków generowania powiadomień w oparciu o kryteria: priorytet alertu, sonda z jakiej napłynął alert, polityka która wyzwoliła alert, grupa do której przypisany jest alert; musi istnieć możliwość tworzenia dowolnej ilości konfiguracji powiadomień w oparciu o wyżej zdefiniowane kryteria z możliwością łączenia parametrów różnych kryteriów w obrębie definicji jednego powiadomienia.	
D-28	System musi posiadać możliwość integracji z rozwiązaniami typu SIEM, oraz eksportu danych przy użyciu protokołów syslog oraz syslog LEEF przy użyciu protokołów UDP, TCP, TLS.	

D-29	System musi posiadać możliwość automatycznego tworzenia i wysyłania raportów przynajmniej w formacie PDF, informujących o statystykach i trendach oferując: 1) Wbudowane wzory raportowania (m.in. podsumowanie wykrytych nieprawidłowości, złośliwego oprogramowania, ataków i wycieku danych, cyklu obsługi incydentów w odniesieniu do statusu alertów w systemie ticketowym). 2) Tworzenie własnych szablonów raportów lub modyfikacji już istniejących przy użyciu edytora dostępnego w panelu Systemu, w oparciu o możliwość przeszukiwania, filtrowania, grupowania, wyznaczania trendów i zliczania danych zebranych w Systemie w postaci alertów, jak również urządzenia pamięci sieciowej 3) Przesyłanie wygenerowanych raportów do wybranych adresatów poczty elektronicznej.	
D-30	System musi posiadać dostępny na żądanie formularz umożliwiający ręczne przeszukiwanie i grupowanie alertów według kryteriów bazujących na własnościach lokalizacji i kanałów komunikacji z możliwością bieżącej modyfikacji tych kryteriów. System musi umożliwiać tym zakresie: 1) Stosowanie operacji logicznych (co najmniej OR i AND); 2) Wielopoziomowego zagnieżdżania warunków; 3) Stosowanie w zapytaniach wyrażeń regularnych, relacji zawierania, możliwości podawania listy wartości w jednym polu zapytania, weryfikacji czy dane pole posiada przypisaną jakąkolwiek wartość.	
D-31	System musi umożliwiać otwieranie zapisanych danych śledczych bezpośrednio z interfejsu zarządzania w kontekście wygenerowanego zdarzenia oraz musi oferować podgląd zdekodowanej treści w obrębie okna zdarzenia (np. widok treści przekonwertowanego do czystego tekstu dokument MS Excel; pobranie dokumentu MS Excel; możliwość pobrania archiwum ZIP, którego jednym z elementów był plik MS Excel naruszający zdefiniowane w polityce warunki).	
D-32	Dla polityk zapisujących surowy ruch sieciowy powiązany z naruszeniem widok alertu musi posiadać możliwość wizualizacji i filtrowania surowych danych (PCAP) oraz możliwość ich pobrania z poziomu panelu Systemu.	
D-33	System musi posiadać możliwość tworzenia własnych pulpitów (dashboard) i widoków oraz modyfikacji już istniejących.	
D-34	System musi umożliwiać zapisanie wykonywanych zapytań i widoków grupowania alertów w celu ich ponownego użycia w przyszłości oraz oferować możliwość prezentowania danych z zapisanych widoków w postaci wykresów obrazujących trendy.	
D-35	System musi prezentować w formie graficznej podsumowanie zidentyfikowanych typów zagrożeń z podziałem na kategorie: wyciek danych, skompromitowane maszyny, złośliwe oprogramowanie, podejrzane hosty, proaktywne rozpoznanie, prezentując podsumowanie z ustalonego przez operatora zakresu czasu (przynajmniej 30 dni) wykorzystując dane zgromadzone na urządzeniu zarządzającym i urządzeniu pamięci sieciowej.	
D-36	Wymagane jest, aby oferowany System umożliwiał zdalny dostęp administracyjny przy użyciu protokołu SSH do każdego komponentu Systemu (np. w celach diagnostycznych).	
D-37	System musi umożliwiać określanie krytyczności alertów wyświetlanych w interfejsie.	
D-38	Alerty o różnej krytyczności muszą być wyraźnie wyróżnione (np. kolorystycznie).	
D-39	Zawartość bazy danych systemu zarządzania musi być zaszyfrowana.	
D-40	System musi umożliwiać testowanie polityk bez wpływu na ruch sieciowy przed ich wdrożeniem produkcyjnym.	
D-41	System musi umożliwiać modyfikacje, dostrajanie i tworzenie wyjątków w politykach dostarczanych przez producenta.	
D-42	Moduł zarządzania musi przechowywać i udostępniać informacje audytowe o wszystkich zmianach w konfiguracji.	

D-43	Moduł zarządzający musi być wyposażony w podstawowy system obsługi incydentów (przypisywanie do użytkownika, przekazywanie, dodawanie notatek, przypisywanie wielu zdarzeń do jednego incydentu itp.).	
D-44	System zarządzania musi udostępniać materiał analityczny związany ze zdarzeniami w formie, która gwarantuje integralność tego materiału.	
D-45	Moduł zarządzania musi być wyposażony konfigurowalny w panel kontrolny umożliwiający ocenę sytuacji pod względem stanu systemu, ilości wykrytych zagrożeń, statystyk itp.	
D-46	System musi umożliwiać ograniczenie dostępu do raportów ze względu na role (RBA).	
D-47	System musi umożliwiać automatyczne generowanie raportów w predefiniowanym wyznaczonym czasie.	
D-48	System musi umożliwiać przesyłanie wygenerowanych raportów do wybranych adresatów poczty elektronicznej.	
D-49	System musi umożliwiać automatyczne, selektywne przesyłanie informacji o zdarzeniach za pośrednictwem protokołu syslog.	
D-50	System musi umożliwiać automatyczne, selektywne przesyłanie informacji o zdarzeniach za pośrednictwem poczty e-mail.	
D-51	System musi umożliwiać automatyczne, selektywne przesyłanie informacji o zdarzeniach za pośrednictwem protokołu SNMP.	
D-52	System musi umożliwiać dostęp do informacji o zdarzeniach za pośrednictwem API.	
D-53	System musi umożliwiać tworzenie raportów dostosowanych do potrzeb użytkownika.	
D-54	System musi pozwalać na tworzenie polityk bezpieczeństwa, które umożliwią na wykrycie określonych typów i struktur danych przesyłanych w ruchu sieciowym, a w konsekwencji identyfikacji przypadków wycieku danych lub propagacji złośliwego oprogramowania. Informacja o wykryciu naruszenia polityki i podjętym działaniu powinna być przesłana do wskazanych użytkowników Systemu w zależności od konfiguracji mechanizmów alarmowania/powiadamiania.	
D-55	System musi pozwalać na definiowanie alertów, pozwalających na minimum wysłanie wiadomości e-mail do administratora w przypadku wykrycia niepożądanego ruchu.	
D-56	System musi posiadać możliwość wizualizacji trendów oraz nawigowania przez wyniki zapytań z wykorzystaniem histogramów i innych sposobów graficznego zobrazowania ich wyników.	
D-57	System musi umożliwiać automatyczne rejestrowanie wszystkich informacji o ruchu sieciowym, który przechodzi przez sondę systemu niezależnie od konfiguracji polityk systemu. Rejestrowanie musi być realizowane przez urządzenie wyposażone w przestrzeń dyskową, która umożliwi przechowywanie danych co najmniej przez okres 90 dni. Informacje o rejestrowanym ruchu muszą być zapisywane w dedykowanej, wydajnej bazie danych. Rejestrowane dane muszą zawierać informacje o parametrach sesji we wszystkich warstwach sieciowych: adresy i porty komunikacyjne, informacje o protokołach komunikacji i aplikacjach, informacje o atrybutach aplikacji i protokołów, informacje o zawartości komunikacji (nazwy i metadane plików). Wymagane jest, aby rejestrowane były jedynie metadane komunikacji sieciowej, bez konieczności zapisywania całego ruchu sieciowego (wraz z zawartością).	

Tabela nr 1 – Wymagania funkcjonalne dla Systemu NDR.

2. Wymagania pozafunkcjonalne dla Systemu NDR.

Pola w kolumnie „Opis spełnienia wymagań" wypełnia Wykonawca. Zamawiający oczekuje wskazania do odniesienia w specyfikacji producenta opublikowanej na stronie producenta lub załączonej do oferty specyfikacji producenta potwierdzającej spełnienie wymagań.

Lp.	Wymagania pozafunkcjonalne dla Systemu NDR	Opis spełnienia wymagań
E-1	System musi realizować wszystkie funkcjonalności związane z wykrywaniem i ochroną przed złośliwym oprogramowaniem, zagrożeniami Advanced Persistent Threat (APT), wyciekiem danych, rejestrowaniem zapisów danych z naruszeń, agregowaniem informacji o ruchu sieciowym w sposób nieselektywny przy założeniu, że natężenie analizowanego ruchu wyniesie do 1 Gbps na styku sieci.	
E-2	System musi mieć możliwość działania w trybie HA Active-Passive.	
E-3	Komponenty Systemu odpowiedzialne za funkcje bezpieczeństwa muszą mieć możliwość skonfigurowania w trybie in-line (L2).	
E-4	Wszystkie sprzętowe komponenty Systemu muszą posiadać redundantne zasilanie.	
E-5	System musi umożliwiać zasilanie ze źródeł zmiennoprądowych 230V (zasilacza AC).	
E-6	System musi zajmować maksymalnie 12U w standardowej szafie rackowej.	
E-7	Centralny system zarządzania musi posiadać redundantne zasilanie.	
E-8	Awaria sondy pracującej wpiętych in-line nie może powodować niedostępności usług sieciowych.	
E-9	Sondy muszą mieć możliwość działania na zasadzie pasywnego nasłuchu ruchu przekierowywanego do nich przy pomocy urządzeń typu TAP lub za pomocą mirroringu portów na przełącznikach sieciowych pod warunkiem zapewnienia funkcjonalności blokowania ruchu naruszającego ustalone polityki ochrony przed wyciekiem danych oraz propagacją oprogramowania złośliwego.	
E-10	Wszystkie sprzętowe komponenty Systemu muszą być wyposażone w dedykowany min. 1 port sieciowy RJ45 przeznaczony do ich konfiguracji i zarządzania.	
E-11	Wszystkie sprzętowe komponenty Systemu muszą być wyposażone w min. 4 porty sieciowe 1 GbE.	
E-12	Wykonawca zapewni dostęp oraz możliwość aktualizacji Zamawiającemu do najnowszych wersji oprogramowania oraz mikrokodów (firmware) dla dostarczonych urządzeń wraz ze wszystkimi ich komponentami, podzespołami, elementami w okresie trwania gwarancji.	
E-13	System musi być kompletny, tj. musi posiadać wszystkie niezbędne elementy sprzętowe (hardware konieczny do uruchomienia Systemu NDR zgodnie z wymaganiami), programowe oraz licencyjne.	
E-14	W ramach gwarancji sprzętowej Wykonawca zapewnia naprawę uszkodzonych komponentów Systemu NDR w miejscu instalacji (on-site).	
E-15	W przypadku awarii nośniki danych zawierające dane przetwarzane u Zamawiającego a stanowiące komponenty Systemu NDR będą zatrzymane przez Zamawiającego.	

Tabela nr 2 – Wymagania pozafunkcjonalne dla Systemu NDR.

Załącznik nr B

1. Wymagania dla Systemu EDR.

Pola w kolumnie „Opis spełnienia wymagań" wypełnia Wykonawca. Zamawiający oczekuje wskazania do odniesienia w specyfikacji producenta opublikowanej na stronie producenta lub załączonej do oferty specyfikacji producenta potwierdzającej spełnienie wymagań.

Lp.	Wymagania funkcjonalne dla Systemu EDR	Opis spełnienia wymagań
F	**Wykrywanie i reagowanie na nieznane zagrożenia**	
F-1	Oprogramowanie agenta musi mieć możliwość zbierania wszystkich zdarzeń z systemów MS Windows takich jak: 1) Zmiany w rejestrze; 2) Operacje na poziomie procesów (tworzenie, zamykanie, etc); 3) Operacje na poziomie plików (tworzenie, kasowanie, modyfikacja, etc); 4) Operacje na poziomie pamięci masowej podłączanej po USB; 5) Operacje na poziomie zapytań DNS; 6) Operacje na poziomie komunikacji sieciowej; 7) Wskazane zdarzenia zbierane przez log systemowy.	
F-2	Agent musi implementować reguły wykrywania potencjalnych nowych zagrożeń na poziomie analizy zbieranych zdarzeń opisanych powyżej.	
F-3	Reguły behawiorystyczne muszą być dostarczane i tworzone przez producenta systemu.	
F-4	Musi istnieć możliwość tworzenia reguł własnych np. na podstawie zebranych zdarzeń.	
F-5	Musi istnieć możliwość zatrzymania procesu albo drzewa procesów w przypadku naruszenia zdefiniowanej reguły behawiorystycznej.	
F-6	Musi istnieć możliwość zbierania zdarzeń tylko w oknie wystąpienia alarmu tj. 2 minuty przed oraz po alarmie. Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręcznie bądź z Active Directory.	
F-7	Agent musi umożliwiać szereg reakcji uruchamianych ręcznie bądź automatycznie na podstawie generowanych alarmów, takich jak: 1) Analiza pamięci; 2) Zrzut pamięci oraz zrzut obrazu dysku; 3) Zebranie wskazanego pliku; 4) Przeszukanie rejestru; 5) Zebranie informacji z ARP cache; 6) Zebranie informacji z DNS cache; 7) Odtworzenie systemu operacyjnego w całości; 8) Powrót do ostatniej dobrej konfiguracji; 9) Zakończenie wskazanego procesu; 10) Lista zalogowanych użytkowników; 11) Zebranie informacji o zadaniach, ustawieniach autorun, etc.	
F-8	Musi istnieć możliwość tworzenia własnych zadań wykonywanych przez agenta w formie skryptu wraz z ewentualnymi narzędziami potrzebnymi do jego wykonania	
F-9	Musi istnieć możliwość ręcznej oraz automatycznej izolacji hosta na skutek wykrytego zdarzenia.	
F-10	Musi istnie wywołania zdalnej konsoli oraz przeglądarki plików i procesów z najwyższymi uprawnieniami	
F-11	Musi istnieć możliwość określenia adresów IP zaufanych serwerów z którymi komunikacja jest zawsze dozwolona (np. Active Directory/Kontrolery domeny/etc)	
F-12	Agent musi pozwalać na blokowanie uruchamiania się procesów o wskazanych sumach kontrolnych. Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręcznie bądź z Active Directory.	
F-13	Agent musi pozwalać na odkładanie każdej nowej instancji kodu wykonywalnego widzianego pierwszy raz w środowisku nawet jeżeli kod ten nie zostanie zapisany w formie pliku na dysku (np. skrypt uruchamiany	

	w pamięci). Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręczenie bądź z Active Directory	
F-14	Agent musi pozwalać na uruchamianie i analizę plików YARA oraz IOC. Producent musi udostępniać uaktualnianą listę plików oraz musi istnieć możliwość wskazania serwera z własnymi listami. Musi również być możliwość importu własnych plików.	
F-15	Musi istnieć możliwość wykonywania (detonacji) zbieranych próbek plików wykonywalnych w sposób automatyczny i ręczny w zainstalowanym lokalnie komponencie piaskownicy Systemu NDR. Minimalna ilość detonacji to 8000 w ciągu 24 godz. Detonacja plików musi przebiegać w środowisku Zamawiającego.	
F-16	Agent musi zbierać informacje o zainstalowanym oprogramowaniu na hoście oraz korelować ją z listą aktualnych znanych podatności (CVE) wskazując istniejące podatności na każdym z hostów.	
F-17	Cała opisana funkcjonalność w zakresie wykrywania i reagowania na nieznane zagrożenia musi być dostępna na systemy klasy: 1) MS Windows 10 i nowszych; 2) MS Server 2012 i nowszych; 3) Linux (Centos, Debian, RHLE); 4) macOS.	
G	**Zarządzanie systemem**	
G-1	System musi pozwalać na zarządzanie wszystkimi komponentami dokonującymi analizy oraz wszystkimi ich parametrami takimi, jak: 1) konfiguracja trybów pracy; 2) tworzenie reguł/polityk bezpieczeństwa; 3) konfigurację zasad alarmowania; 4) zasad eksportu danych do innych systemów bezpieczeństwa; 5) zasad wykonywania kopii bezpieczeństwa; 6) propagowanie poprawek i aktualizacje oprogramowania; 7) zarzadzanie licencjami przy pomocy komponentu realizującego funkcję centralnego systemu zarządzania.	
G-2	Korzystanie z centralnego systemu zarządzania musi odbywać się przy pomocy jednego interfejsu graficznego dostępnego zdalnie, przy wykorzystaniu przeglądarki internetowej.	
G-3	Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu EDR jak również pomiędzy poszczególnymi jego komponentami musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.	
G-4	Centralny system zarządzania musi pozwalać na tworzenie kont użytkowników Systemu EDR o różnych poziomach uprawnień. W zakresie uwierzytelniania użytkowników Systemu EDR wymagana jest możliwość integracji z LDAP/AD.	
G-5	W ramach konsoli zarządzającej, dla wszystkich obsługiwanych przez nią komponentów, musi być dostępna funkcjonalność wewnętrznego audytu, umożliwiająca logowanie i przegląd wszystkich działań.	
G-6	Musi istnieć możliwość integracji z systemami klasy SIEM celem wysyłania informacji o zdarzeniach do dalszej korelacji.	
G-7	Musi istnieć możliwość integracji poprzez API z systemami SOAR celem automatyzacji konfiguracji.	

Tabela nr 1 – Wymagania funkcjonalne dla Systemu EDR.

Bankowy Fundusz Gwarancyjny

Załącznik C

1. Dodatkowe nieobligatoryjne wymagania dla Systemu EDR.

Jeśli System EDR będzie spełniać wszystkie dodatkowe nieobligatoryjne wymagania funkcjonalne opisane w tabeli nr 1 oferta Wykonawcy otrzyma dodatkowe punkty.

Pola w kolumnie „Opis spełnienia wymagań" wypełnia Wykonawca. Zamawiający oczekuje wskazania do odniesienia w specyfikacji producenta opublikowanej na stronie producenta lub załączonej do oferty specyfikacji producenta potwierdzającej spełnienie wymagań.

Lp.	Dodatkowe nieobligatoryjne wymagania funkcjonalne dla Systemu EDR	Opis spełnienia wymagań
H	**Ogólne wymagania nieobligatoryjne**	
H-1	System EDR powinien zapewniać automatyczną analizę i wizualizację ataku (w tym opracowanie harmonogramu zdarzeń i wstępnej oceny dotkliwości/wpływu).	
H-2	System EDR musi zapewniać zintegrowaną analitykę (w tym wizualizację) i wspierać tworzenie niestandardowej analityki w celu zidentyfikowania anomalii zachowań punktów końcowych, wsparcia badania incydentów i analizy zdarzeń.	
H-3	System EDR powinien mieć możliwość automatycznej izolacji pliku/aplikacji/hosta w momencie wykrycia potencjalnego zagrożenia lub interakcji z treściami, które może stanowić zagrożenie dla infrastruktury Zamawiającego	
H-4	Rozwiązanie powinno obsługiwać szybkie rozsyłanie (w ciągu maks. kilku minut) zmian konfiguracji z serwera zarządzania do wszystkich zainstalowanych agentów Systemu EDR	
H-5	Możliwość odinstalowania rozwiązania powinno zapewniać, że po wykonaniu procesów odinstalowywania nie pozostaną żadne zależności/artefakty, które będą wpływać na poprawne działanie systemu stacji końcowej.	
H-6	Rozwiązanie musi automatycznie zgłaszać wykrycie potencjalnie złośliwych zdarzeń do serwera zarządzania. Notyfikacja zewnętrzna (wysyłanie powiadomień poza organizację) wykrywanych zdarzeń musi mieć charakter manualny i wymagać zgody administratora systemu.	
H-7	Centralny system zarządzania musi być wspólny dla Systemu EDR i Systemu NDR. Z poziomu wspólnego systemu zarzadzania musi być możliwy przegląd zdarzeń wykryty przez dostarczany System EDR i System NDR, a także musi być możliwość podejmowania działań naprawczych i/lub diagnostycznych.	
H-8	System EDR, za pośrednictwem centralnego serwera zarządzania, musi zapewnić opcje konfigurowania automatycznych lub ręcznych działań naprawczych w odpowiedzi na wykryte potencjalnie złośliwe zdarzenia dla wszystkich urządzeń, wybranej grupy urządzeń, urządzeń podatnych, urządzeń zainfekowanych, wybranych urządzeń.	
H-9	Informacje dotyczące aktualizacji/modyfikacji oprogramowania, np. wersja oprogramowania, znaczniki identyfikacyjne oprogramowania, informacje o łatce aktualizacyjnej.	
H-10	Informacje na temat zdefiniowanych zmian mających wpływ na konfigurację sieci na stacji końcowej.	
H-11	Możliwość wykrywania podpiętych urządzeń zewnętrznych z wykorzystaniem interfejsu bezprzewodowego np. WiFi, Bluetooth.	

Tabela nr 1 – Dodatkowe nieobligatoryjne wymagania funkcjonalne dla Systemu EDR.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl