ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI III

I. Nazwa zamówienia

Rozbudowa systemu IBM QRadar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją

I.1 **Kody CPV**

32420000-3 Urządzenia sieciowe.
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.

II. Przedmiot zamówienia

(1) Przedmiot zamówienia obejmuje dostawy licencji oraz sprzętu, dotyczące systemu IBM Qradar, opisane w pkt III.1 oraz III.2, a następnie świadczenie usług opisanych w pkt. III.3 – III.5.

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Dzień Roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Godziny ekspercie	usługi konsultacji (tzw. ang. *Professional Services*), których przedmiotem będą miedzy innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji i eksploatacji SIEM QRadar, bieżących problemów dotyczących funkcjonowania SIEM QRadar, konsultacji, na warunkach wskazanych w OPZ, w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.
Hardware Appliance	ang. Hardware Appliance oznacza sprzęt fizyczny, do którego Producent dostarcza wsparcie techniczne.
Roboczogodzina	jedna godzina pracy członka personelu Wykonawcy.
Urządzenie	oznacza przedmiot zamówienia opisany w pkt. III.2 niniejszego dokumentu.
Wsparcie producenta	oznacza oferowane przez producenta danego rozwiązania aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu.

(3) Przedmiot zamówienia został opisany przez wskazanie znaków towarowych, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy "lub równoważny".

(4) W opisie przedmiotu zamówienia Zamawiający w zakresie każdego wskazania wymienionego w powyższym pkt 1 wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne wszystkich kryteriów równoważności.

(5) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym, i takim odniesieniom towarzyszą wyrazy "lub równoważne".

(6) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

(7) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

(8) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przyapdkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(9) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

(10) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.

(11) Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.

III. Specyfikacja wymagań

(1) Przedmiotem zamówienia jest rozbudowa systemu klasy SIEM firmy IBM - QRadar, posiadanego przez Zamawiającego, dalej określanego również jako „SIEM QRadar”. Wykonanie przedmiotu

zamówienia obejmuje dostawę licencji oraz sprzętu, opisanych w pkt III. 1 i III. 2 poniżej, a następnie świadczenie usług, opisanych w pkt III. 3, III. 4, III.5 poniżej.

III.1 **Dostawa licencji**

(1) Zamawiający wymaga dostarczenia licencji do rozbudowy posiadanego przez Zamawiającego systemu SIEM QRadar, zgodnych z poniższym opisem:

lp.	Opis licencji	Ilość
1	min. 20tys. EPS (ang. Event Per Second). Licencja lub licencje: IBM QRadar Event Capacity Events Per Second License lub równoważne.	n.d.
2	min. 10 tys. FPM (ang. Flow Per Minute). Licencja lub licencje: IBM QRadar Flows Capacity Flows Per Minute License lub równoważne.	n.d.
3	HA (ang. High Availability), która umożliwi wysoką dostępność komponentu SIEM. Licencja: IBM QRadar High Availability Software Install License lub rówoważne.	1
4	Licencje umożliwiające implementacje komponentu SIEM Licencje: IBM QRadar Software Node Install License lub rówoważne.	6

(2) Zamawiający dopuszcza jako „licencje równoważne" licencje zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o posiadane przez Zamawiającego licencje, wymienione powyżej. W przypadku dostarczenia licencji równoważnych Wykonawca zapewni asystę techniczną Zamawiającemu lub podmiotowi wskazanemu przez Zamawiającego w celu dokonania ich implementacji w posiadanym przez Zamawiającego środowisku. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania opisane poniżej.

III.1.1 **Kryteria stosowane w celu oceny równoważności:**

(1) Zamawiający wskazuje, że zgodnie z przepisem art. 99 ust. 5 PZP dokonał opisu przedmiotu zamówienia poprzez wskazanie produktu referencyjnego oraz określenie następujących parametrów równoważności

(2) **AD.1** Licencja dot. EPS zwiększy liczbę o 20 tysięcy przyjmowanych zdarzeń na sekundę w czasie rzeczywistym. Pozwoli to na podłączenie większej ilości systemów do SIEM QRadar i zwiększy możliwości obsłużenia ilości zdarzeń, które są generowane przez te systemy. Systemy produkują zdarzenia z różną intensywnością (w danym czasie na sekundę) w zależności od rodzaju i użycia.

a. Zamawiający szacuje liczbę systemów będących pod monitoringiem systemu SIEM QRadar, pod względem zdarzeń, na poziomie min. 500 sztuk.

(3) **AD.2** Licencja dot. FPM zwiększy liczbę o 10 tysięcy przyjmowanych przepływów (ang. Flow) na minutę w czasie rzeczywistym, pochodzących z urządzeń sieciowych. Pozwoli to na

monitorowanie większej ilości przepływów min. w formacie: NetFlow, IPFIX, sFlow, J-flow i zwiększy możliwość obsłużenia ilości przepływów na minutę, które są generowane przez urządzenia sieciowe.

b. Zamawiający szacuje liczbę urządzeń sieciowych będących pod monitoringiem systemu SIEM QRadar i wysyłających przepływy (ang. flow) na poziomie min. 100 sztuk.

(4) **AD.3** Licencja HA umożliwią zachowanie ciągłości działania w przypadku awarii jednego wybranego przez Zamawiającego zaimplementowanego komponentu SIEM QRadar. Komponenty SIEM QRadar mogą pracować w trybie active / standby. W przypadku awarii komponentu aktywnego dzięki licencji HA nastąpi przełączenie komponentu będącego w trybie standby na aktywny co zminimalizuje ryzyko utratu ciągłości działania wybrango komponentu SIEM QRadar.

(5) **AD.4** Licencja umożliwi implementacje dowolnego komponentu SIEM QRadar w trybie aktywnym lub standby np. tj. konsola, procesor, kolektor, itp. Jest to licencja wymagana przez IBM, która umożliwi legalne korzystanie z w/w komponentu SIEM Qradar i umożliwi wsaprcie techniczne Producenta.

(6) Dostarczone licencje równoważne nie mogą ograniczać obecnej funkcjonalności SIEM QRadar w tym:

- zdolność do zbierania logów z dowolnych systemów i urzedzeń sieciowych, w celu ich przechowywania, normalizacji i analizy,
- zdolność adaptacji/rekonfiguracji/przystosowania SIEM QRadar do współpracy z różnymi rozwiązaniami bezpieczeństwa,
- zdolność do przekazania dalej skorelowanej informacji o wykrytym ataku lub działaniu niepożądanym do innych rozwiązań bezpieczeństwa i urządzeń sieciowych.

III.2 **Dostawa Sprzętu**

(1) Zamawiający, w celu wykonania rozbudowy posiadanego przez Zamawiającego systemu SIEM QRadar, producenta IBM, wymaga dostarczenia **<u>dwóch</u>** urządzeń, zgodnych z poniższym opisem:

LP.	Opis	Ilość (sztuki)
1	Sprzęt: IBM Hardware Appliance model Lenovo System SR650 M6 (Qradar XX29 G2 lub równoważny lub nowszy) w raz z: • odpowiednimi licencjami umożliwiającymi uruchomienie komponentu Event i Flow Procesora, który obsłuży EPS na poziomie min. 15tys. i 300 tys. FPM. • zestawem montażowym w szafie RACK. • kompatybilnymi (z zainstalowanymi kartami sieciowymi) wkładkami.	2
2	**Dodatkowe:** Urządzenia muszą być fabrycznie nowe oraz nie mogą znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025.	

III.2.1 **Kryteria stosowane w celu oceny równoważności:**

(2) Zamawiający wskazuje, że zgodnie z przepisem art. 99 ust. 5 PZP dokonał opisu przedmiotu zamówienia poprzez wskazanie produktu referencyjnego oraz określenie następujących minimalnych parametrów równoważności dla każdego z dwóch sztuk sprzętu (n/w podzespoły mają zachowają kompatybilność między sobą).

Parametr	Wartości minimalne:
Procesor	Dwa procesory nie mniej niż 12-rdzeniowe z rodziny x86 (64 bitowe)
Pamięć RAM	256 GB
Dyski	12 x 8 TB 7.2 K 12 Gbps NL SAS 930-16i 4 GB. Powyższe konfiguracje dyskowe muszą być realizowane za pomocą min. jednego sprzętowego kontrolera RAID.
Karty sieciowe	1. 2 x 10 GbE SFP+ wraz z kompatybilnymi wkładkami SFP+10GBase-SR. 2. 4x 1 Gb Ethernet. 3. 1 x RJ-45 10/100/1000 Mb Ethernet na potrzeby systems management (IMM) port 4. 2 x 16 Gbps Fibre Channel SFP+ wraz z kompatybilnymi wkładkami.
Wspierane oprogramowanie (ang. OS)	Sprzęt musi umożliwić uruchomienie i poprawne funkcjonowanie 64-bitowego systemu operacyjnego typu: RHEL v7.3 oraz oprogramowanie firmy IBM: QRadar® w wersji 7.3.3 i 7.4.
Zasilanie	Dwa (dla redundancji) zasilacze AC o mocy odpowiedniej dla powyższej specyfikacji (każdy nie mniej niż 750 W AC).
Montaż	Obudowa nie większa niż 2U, dedykowana do montażu w szafie Rack 19". Wraz z serwerem muszą być dostarczone niezbędne elementy montażowe do szafy Rack 19".
Dodatkowe	Urządzenia muszą być fabrycznie nowe oraz nie mogą znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025.

III.3 **Zasady świadczenia usług Godzin eksperckich w ramach prawa opcji**

(1) Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący z producentem przedmiotu zamówienia opisanego w pkt III.1 i III.2 powyżej (dalej określanego jako „**Producent**"), w najwyższym poziomie partnerstwa

przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta – w wymiarze łącznie 736 Roboczogodzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1 i III.2 powyżej, do końca grudnia 2022r.

(1) Osoba realizująca usługi w ramach Godzin eksperckich musi być ekspertem w obszarze związanym z zaoferowaną technologią oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką (np. IBM Certified Deployment Professional Security lub IBM Certified Associate Administrator lub nowszym) oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

(2) W ramach usług realizowanych jako Godziny eksperckie będzie m.in. na żądanie Zamawiającego:

(a) opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.1powyżej (z uwzględnieniem wykorzystywanych przez Zamawiajacego komponentów systemu SIEM) oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Godzin eksperckich,

(b) opracowanie i dostarczenie procedury postępowania w razie wystąpienia incydentów bezpieczeństwa w SIEM

(c) opracowanie i dostarczenie procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

(d) konsultacje oraz wsparcie we wdrożeniu oraz konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1 i III.2 powyżej,

(e) wsparcie i konsultacje dot. utrzymania, eksploatowania, tuningu konfiguracji i reguł/polityk bezpieczeństwa oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt III.1 i III.2 powyżej,

(f) montaż w serwerowni Zamawiającego przedmiotu zamówienia, o którym mowa w pkt III.2 powyżej,

(3) Osoby realizujące prace na życzenie Zamawiającego w lokalizacji instalacji Urządzenia będą zobowiązane do dostarczenia aktualnego zaświadczenia o niekaralności lub poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „POUFNE", na min. 7 dni przed rozpoczęciem prac.

(4) Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z Wykonawcą Umowie, wskazujących przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 dni roboczych od dnia przekazania Wykonawcy zlecenia.

(5) Świadczenie usług w ramach Godzin Eksperckich uzależnione jest od wcześniejszego zlecenia ich zakresu przez Zamawiajacego, poprzez złożenie oświadczenia o skorzystaniu z prawa opcji. Skorzystanie z prawa opcji jest uprawnieniem Zamawiającego, z zastrzeżeniem, że korzystając z prawa opcji, nie jest zobowiązany do zakupienia żadnej ilości Godzin eksperckich, a całość tego świadczenia objęta jest prawem opcji, które nie musi być wykonane przez Zamawiajacego. Nieskorzystanie przez Zamawiającego z prawa opcji nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń w stosunku do Zamawiającego.

III.4 **Zasady świadczenia Gwarancji**

(1) Wykonawca zobowiązany jest zapewnić Zamawiającemu Gwarancję dla przedmiotu zamówienia opisanego w pkt III.2 udzieloną przez Producenta Urządzeń (dalej określanego jako „**Producent**”) lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta, obejmującą okres 36 miesięcy, od dnia odbioru sprzętu opisanego w pkt III.2.

(2) Wykonawca, zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu Gwarancji, zgodnie z następującymi zasadami:

(a) Zamawiający będzie uprawniony do dokonywania zgłoszeń awarii w trybie 24/7/365, za pośrednictwem telefonu lub dedykowanej aplikacji lub adresu poczty elektronicznej, wskazanych przez Wykonawcę;

(b) Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy;

(c) Zgłoszone awarie będą usuwane w terminie do końca trzeciego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.

(3) W przypadku w którym usunięcie awarii będzie wymagać odinstalowania urządzenia, które uległo awarii:

(a) Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tą lokalizację;

(b) Wydanie urządzenia poza miejsce jego instalacji, w celu dokonania naprawy, będzie mogło nastąpić dopiero, po trwałym usunięciu danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez gwaranta i zdeponowaniu ich u Zamawiającego;

(4) W przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie określonym w pkt 2c powyżej Wykonawca zobowiązuje się zapewnić urządzenie zastępcze na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie oraz zapewniających nie gorszy poziom bezpieczeństwa. W przypadku zwrotu urządzenia zastępczego, gwarant zapewni trwałe usunięcie danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez gwaranta i zdeponowaniu ich u Zamawiającego. W takim przypadku termin usunięcia awarii przez gwaranta wynosi 30 dni kalendarzowych od chwili zgłoszenia awarii.

gwarant zapewni wsparcie techniczne w stosunku do urządzenia zastępczego do czasu naprawienia urządzenia które uległo awarii.

(5) Gwarant jest zobowiązany do wymiany urządzenia na nowe na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie w przypadku, w którym usunięcie awarii o której mowa w pkt. 4 powyżej jest niemożliwe. W takim przypadku gwarant zapewni wsparcie techniczne w stosunku do nowego urządzenia.

(6) Wykonywanie zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu gwaranta następujących wymogów:

(a) przedłożenia aktualnego zaświadczenia o niekaralności lub poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „POUFNE".

III.5 **Zasady świadczenia usług Wsparcia producenta**

(1) Wykonawca zobowiązany jest zapewnić wsparcie Producenta przedmiotu zamówienia opisanego w pkt III.1 i III.2 powyżej (dalej określanego jako „Producent") lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta dla dostarczonych licencji lub subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt III.1.

(2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy oraz instrumentów zgłaszania błędów.

(3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez Producenta wraz z niezbędnymi danymi logowania, umożliwiającymi samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiającymi zakładanie zgłoszeń serwisowych.

III.6 **Pozostałe wymagania zostały opisane w Projektowanych postanowieniach umowy, które zawarte są w rozdziale III SWZ.**