ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Rozbudowa infrastruktury systemów nadzoru i bezpieczeństwa (5 części).

II. Kody CPV

dla części I: 32424000-1,
dla części II: 72591000-4,
dla części III: 32424000-1,
dla części IV: 48210000-3,
dla części V: 30231300-0, 30214000-2.

III. Przedmiot zamówienia

Część I Dostawa i wdrożenie systemu NGFW;
Część II Przedłużenie wsparcia systemu IPS;
Część III Rozbudowa infrastruktury F5 BIG-IP;
Część IV Rozbudowa infrastruktury DAM;
Część V Dostawa stacji roboczych i monitorów.

Zamawiający dokonał opisu przedmiotu zamówienia z podziałem na pięć części z wykorzystaniem następujących definicji

Nazwa / skrót	Opis
Dzień Roboczy	Oznacza dzień od poniedziałku do piątku niebędący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Osobodzień	Oznacza jednostkę miary czasu wykonywania usług, obejmującą pracę jednej osoby przez 8 godzin, bez ograniczenia Dni Roboczych.
Wsparcie producenta	Oznacza oferowane przez producenta danego rozwiązania aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu.
WAF	Ang. Web Application Firewall oznacza moduł ochrony ruchu webowego realizowany w Urządzeniu F5 BIG-IP 5000 posiadanym przez Zamawiającego.
DAM	Ang. Data Activity Monitor oznacza system IBM Guardium dedykowany do ochrony Baz Danych, posiadany przez Zamawiającego.
IPS	Jeden z modułów bezpieczeństwa w NGFW (ang. Intrusion Prevention system).
Infrastruktura IPS Zamawiającego	Oznacza urządzenia, o których mowa w Części II, opisane przez Zamawiającego w oświadczeniu, przekazywanym Wykonawcom zgodnie z postanowieniami ust. 4 pkt 4.2. Rozdziału I SIWZ .
F5 BIG-IP	Urządzenie fizyczne firmy F5 (F5 BIG-IP 5000) będące w posiadaniu Zamawiającego (2 szt.).

1. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co mogłoby prowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne". Nie dotyczy to sytuacji, w których Zamawiający definiuje posiadaną przez siebie infrastrukturę w celu precyzyjnego określenia środowiska, z którym przedmiot zamówienia ma być kompatybilny.
2. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na normy, europejskie oceny techniczne, aprobaty, specyfikacje techniczne i systemy referencji technicznych, należy odczytywać z wyrazami „lub równoważne". Nie dotyczy to sytuacji, w których Zamawiający definiuje posiadaną przez siebie infrastrukturę w celu precyzyjnego określenia środowiska, z którym przedmiot zamówienia ma być kompatybilny.
3. W przypadku zaoferowania rozwiązania równoważnego, zgodnie z art. 30 ust. 5 ustawy Pzp, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez urządzenia lub oprogramowanie równoważne poszczególnych parametrów równoważności. Zamawiający wymaga realizacji takiego obowiązku w ofercie Wykonawcy.
4. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
5. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury u Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu oprogramowania.

Cześć I – dostawa systemu NGFW

Przedmiotem zamówienia jest dostawa systemu NGFW (ang. Next Generation Firewall), (zwanego dalej „Systemem NGFW") oraz świadczenie usług związanych z dostarczonym Systemem NGFW. Na System NGFW składają się dwa urządzenia NGFW (zwane dalej ,,NGFW"), opisane poniżej i dwie konsole NGFW (zwane dalej ,,Konsola NGFW").

III.1.1 OGÓLNE WYMAGANIA DLA DOSTAWY SYSTEMU NGFW

Lp.	Opis wymagania	Parametry minimalne
1	Parametry montażowe	System NGFW musi składać się z dedykowanych urządzeń fizycznych przystosowanych do montażu w szafach RACK 19" wraz z zestawem montażowym.
2	Zasilacze	2.1. Każde z urządzeń fizycznych wchodzące w skład Systemu NGFW musi być wyposażone w minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. 2.2. Każde z urządzeń fizycznych wchodzące w skład Systemu NGFW musi posiadać takie zasilacze, że w przypadku awarii jednego z nich, drugi zasilacz umożliwi zasilenie w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych.
3	Jednorodność, Szyfrowanie, Dodatkowe kryteria bezpieczeństwa	3.1 Urządzenia wchodzące w skład Systemu NGFW muszą pochodzić od tego samego producenta oraz być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale", „end-of-life" oraz „end-of-support" producenta. 3.2 NGFW musi dostarczać mechanizm szyfrowania danych, który będzie posiadał certyfikacje FIPS 140-2 lub równoważny*. 3.4 Zgodność sprzętu z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym[1]; 3.5. Powinien posiadać zgodność z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym[2].

*Zamawiający wskazuje następujące warunki równoważności dla normy FIPS 140-2 i uzna za normę równoważną opisywanej, normę która:

1) Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
2) Została wydane przez NIST lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,

[1] **Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SIWZ.**
[2] **Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SIWZ.**

3) Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
4) Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

III.1.2 Szczegółowe wymagania dla dostawy NGFW

4	Rodzaj i Ilość	Dwa fizyczne urządzenia klasy NGFW typu hardware appliance.
5	Wydajność	Całkowita wydajność pojedynczego NGFW w trybie ochrony FW (ang. FireWall), IPS (ang. Intrusion Prevention system) i kontroli aplikacji – nie mniejsza niż 20Gbps.
6	Interfejsy	Każde z dwóch urządzeń NGFW musi być wyposażona w: 6.1 Min. 8 interfejsów 10 Gbps SFP+ wraz z kompatybilnymi wkładkami 10GBase-SR (LC) objętymi tą samą gwarancją co NGFW. 6.1.1 Dodatkowo niezbędne są kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.2 Min. 8 interfejsów 1 Gbps SFP. 6.2.1 Wykonawca dostarczy dwa komplety kompatybilnych wkładek objętymi tą samą gwarancją co NGFW, tzn. 8 sztuk 1000Base-T oraz 8 sztuk 1000Base-SX (LC). 6.2.2 Dodatkowo niezbędne są kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.2.3 Dodatkowo niezbędne są kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie RJ-45 UTP CAT5e. 6.3 Min. 1 interfejs 1 Gigabit Ethernet wydzielony port do zarządzania (out-of-band).
7	Niezawodność	NGFW musi mieć możliwość stworzenia klastra typu active/active i active/standby
8	Sieć i routing	Musi umożliwić obsługę protokołów routingu typu OSPF, statyczne, RIP/RIPv2 oraz protokół IP: IPv4, IPv6.
9	Asymetryczność ruchu	9.1 Ruch pomiędzy dwoma ośrodkami przetwarzania danych jest asymetryczny i dwa NGFW muszą mieć możliwość zachowania stanu sesji (musi być możliwość

		skonfigurowania klastra w drugiej warstwie modelu OSI). 9.2 NGFW musi obsługiwać IEEE 802.3ad i agregowanie interfejsów fizycznych z wykorzystaniem protokołu Link Aggregation Control Protocol (LACP).
10	Pamięć wewnętrzna na OS	NGFW musi być wyposażony w co najmniej dwa dyski twarde (na system) w konfiguracji redundantnej (min. RAID1) każdy o pojemności nie mniejszej niż 240GB.
11	Tryb pracy interfejsów sieciowych	Interfejsy sieciowe NGFW muszą działać w: 11.1. Drugiej warstwie modelu OSI – L2. 11.2. Trzeciej warstwie modelu OSI – L3. 11.3. Trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych). 11.4. NGFW musi obsługiwać protokół Ethernet z obsługą sieci VLAN. 11.5. Obsługa łącz typu trunk z włączonym tagowaniem ramek IEEE 802.1Q. 11.6. Musi umożliwić wykonywanie translacji adresów IP (statycznej i dynamicznej).
12	Tryby pracy modułu inspekcji IPS w NGFW	12.1. Aktywny (blokowanie i monitoring). 12.2. Pasywny (IDS).
13	Kontrola aplikacji	13.1. NGFW musi mieć możliwość wykrywania aplikacji w ruchu sieciowym. 13.2. NGFW musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania. 13.3. NGFW musi wykrywać aplikacje m.in. typu P2P , web drive (np. google drive), web mail (np. gmail). 13.4. NGFW musi wykrywać aplikacje tunelowane w protokole HTTP lub HTTPS.
14	Kategoryzacja www	14.1. System musi obsługiwać mechanizm filtrowania stron WWW w zależności od kategorii treści (min. 10 kategorii). 14.2. Baza kategorii stron musi być aktualizowana w sposób automatyczny. 14.3. System musi zapewnić możliwość wykluczenia z inspekcji komunikacji dot. kategorii dodanej do wyjątków. 14.4. Producent systemu NGFW musi umożliwić aktualizowanie kategorii typu TOR, C&C, proxy anonimizujące, złośliwe strony typu Phishing.

15	Ochrona NGFW - funkcjonalność	15.1. NGFW musi posiadać moduł wykrywania i blokowania ataków oparty o sygnatury. Baza sygnatur musi być przechowywana na NGFW i regularnie aktualizowana w sposób automatyczny. 15.2. Możliwość blokowania ruchu sieciowego na podstawie: • adresów IP, • reputacji (IP, domen i URL), • sygnatur modułu inspekcji IPS, • domen, • URL. 15.3. Blokowanie niedozwolonych aplikacji i protokołów sieciowych. 15.4. Musi umożliwiać automatyczne dodawanie Feed-ów z zewnętrznych serwerów oraz bezpośrednio z plików CSV zawierających listy adresów IP, domen, URL. 15.5. Musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 15.6. Ochrona przed atakami typu flood: • SYN (w tym TCP) floods, • UDP (w tym DNS query) floods, • IP floods, • ICMP floods, • HTTP floods Anomalie dot. floods związanymi z niestandardowymi pakietami. 15.7. Ochrona przed atakami typu „Drive-by-download”. 15.8. Możliwość ochrony przed exploitami i blokowanie ruchu sieciowego z nim związanego w celu ochrony podatnych aplikacji. 15.9. Ochrona przed atakami typu IP Spoofing. 15.10. Ochrona typu anty-Spyware (w ruchu sieciowym). 15.11. Musi umożliwić ochronę (np. „virtual patching” na poziomie sieci) przed próbami wykorzystania podatności (luk) w chronionych systemach. 15.12. Musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

		15.13. Musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). 15.14. Musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. 15.15. Wykrywanie zagrożeń tj. skanowanie sieci, próby przepełnienia bufora, ataki na podatne aplikacje i infrastrukturę. 15.16. Musi być możliwość dodawania wyjątków dot. w/w ochrony per IP / strefa bezpieczeństwa. 15.17. Musi umożliwiać tworzenie polityk bezpieczeństwa w oparciu o mechanizmy geolokalizacji. Baza geolokalizacji musi być aktualizowana w sposób automatyczny (min. raz w mieisiącu przez producenta NGFW).
16	Ochrona NGFW - możliwe reakcje na wykryte zdarzenia bezpieczeństwa w przetwarzanym ruchu sieciowym	16.1. Monitoring z alertowaniem. 16.2. Blokowanie. 16.3. Bez inspekcji (aby wybrany na podstawie IP ruch nie był przesyłany do silnika inspekcji NGFW). 16.4. Dla wskazanych IP (podsieci) lub stref bezpieczeństwa musi być możliwość definiowania różnych (16.1-16.3) w/w reakcji.
17	Komunikacja szyfrowana	17.1 Musi mieć możliwość przesyłania ruchu zaszyfrowanego (co najmniej TLS/SSL) do zewn. deszyfratora. 17.2 Musi mieć możliwość definiowania różnych polityk bezpieczeństwa w kontekście ruchu szyfrowanego. 17.3 Możliwość deszyfrowania ruchu (co najmniej TLS/SSL w oparciu o zaimportowanie klucza prywatnego) oraz szyfracji ruchu z powrotem.

III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW

18	Rodzaj	Dwie Konsole NGFW muszą działać na fizycznych urządzeniach (ang. hardware appliance)
19	Wymagania funkcjonalne	19.1. Konsola NGFW musi umożliwić zarządzanie NGFW (konfiguracja i utrzymanie) oraz

		szczegółową analizę zdarzeń bezpieczeństwa oraz tworzenie Dashboard w ich kontekście. 19.2. Musi umożliwiać generowanie raportów związanymi ze zdarzeniami bezpieczeństwa co najmniej w formatach html, pdf. 19.3. Musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia zewnętrznego. 19.4. Musi pozwalać na automatyczne usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu i po zarejestrowaniu problemów z miejscem na dysku. 19.5. Musi umożliwiać sprawdzenie wpływu na chroniony ruch sieciowy, nowo pobranych sygnatur IPS przed ich zatwierdzeniem. 19.6. Musi umożliwić zarządzanie co najmniej 6-cioma NGFW (jeśli istnieje ograniczenie na ilość podłączanych NGFW do Konsoli NGFW). 19.7. Zarządzanie urządzeniami systemu musi odbywać się za pomocą graficznej konsoli GUI i linii poleceń (CLI). Interfejs systemu musi być w języku polskim lub angielskim. 19.8. Musi pozwalać na zdefiniowanie min. 20 użytkowników o różnych uprawnieniach, pracujących równolegle. 19.9. Musi być możliwe uwierzytelnienie i autoryzacja użytkowników za pośrednictwem protokołów RADIUS i LDAP. 19.10. Musi umożliwiać (w zakresie NGFW i konsoli) budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji. 19.11. Musi umożliwiać logowanie aktywności administratora, zmian konfiguracji (w konsoli i NFGW). Logowanie to musi być realizowane z możliwością wysyłania logów do SIEM (nie może być żadnych limitów licencyjnych z tym związanych). 19.12. Musi umożliwiać zbieranie zarejestrowanych zdarzeń bezpieczeństwa oraz inf. dot. połączeń (z chronionego ruchu sieciowego)

		przechodzących przez w/w NGFW (nie może być żadnych limitów licencyjnych z tym związanych prócz limitów dot. pojemności dyskowej /wydajnościowych) i musi być możliwość wysyłania tych informacji do systemu klasy SIEM (wraz z adresem IP zawartym w polu XForwarded-For).
20	Pojemność dyskowa	20.1. Musi zapewniać przestrzeń dyskową na dane o pojemności nie mniejszej niż 1,6 TB (min. RAID1). 20.2. Konsola NGFW nie może być w żaden sposób limitowana, jeśli chodzi o ilość danych. Może ją jedynie ograniczać ilość zasobów dyskowych Konsoli NGFW. 20.3. Musi być możliwość uruchomienia automatycznej rotacji logów w przypadku przekroczenia max. przestrzeni dyskowej.
21	Niezawodność	21.1. Wymaga się dostarczenia dwóch Konsol NGFW w celu zachowania redundancji. 21.2. Musi być umożliwiony mechanizm zapewniający redundancje w przypadku awarii jednej z dwóch Konsoli Zarządzających (active/active lub active/standby). 21.3. Niedostępność Konsoli NGFW nie może powodować problemów z ruchem przetwarzanym przez NGFW. NGFW muszą realizować przetwarzanie ruchu zgodnie z ostatnią zachowaną konfiguracją.

III.1.4. ZASADY ŚWIADCZENIA USŁUG PROFESJONALNYCH

1. Zamawiający wymaga zapewnienia przez Wykonawcę Usług Profesjonalnych świadczonych bezpośrednio przez producenta przedmiotu zamówienia opisanego w pkt III.1.1, III.1.2, III.1.3 powyżej (dalej określanego jako „**Producent**”) lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta na rynku geograficznym właściwym dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**”) – w wymiarze łącznie 40 osobodni, przez okres 36 miesięcy od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1.1, III.1.2, III.1.3 powyżej.
2. Osoba/y realizująca Usługę Profesjonalną musi być ekspertem w obszarze związanym z technologią NGFW oraz legitymować się ważnym i aktualnym certyfikatem Producenta

lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

3. W ramach Usług Profesjonalnych będzie m.in.:

   3.1. Opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.1.1, III.1.2, III.1.3 powyżej oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Usług Profesjonalnych;

   3.2. 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;

   3.3. Wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1.1, III.1.2, III.1.3 powyżej;

   3.4. konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt III.1.1, III.1.2, III.1.3 powyżej.

4. Osoby realizujące prace w lokalizacji Zamawiającego będą zobowiązane do dostarczenia aktualnego zaświadczenia o niekaralności, na min. 7 dni przed rozpoczęciem prac.

5. Zamawiający wymaga zapewnienia realizacji Usług Profesjonalnych, 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.

III.1.5. ZASADY ŚWIADCZENIA USŁUG GWARANCJI

1. Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla przedmiotu zamówienia opisanego w pkt III.1.1, III.1.2, III.1.3, udzieloną przez Producenta tych urządzeń (dalej określanego jako „**Producent**”) lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**”), obejmującą okres 36 miesięcy, od dnia odbioru sprzętu opisanego w pkt III.1.1, III.1.2, III.1.3.

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

   2.1. 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;

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

2.3. Zgłoszone awarie będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.

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

3.1. Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tę lokalizację;

3.2. 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;

3.3. Wykonawca zobowiązuje się zapewnić urządzenie zastępcze, o parametrach nie gorszych niż naprawiane urządzenie, w przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie jednego Dnia Roboczego od dnia zgłoszenia. 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.

4. Gwarant jest uprawniony do wymiany urządzenia na nowe, w przypadku w którym usunięcie awarii wymaga udostępnienia urządzenia zastępczego.

5. Wykonywania zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu gwaranta następujących wymogów:

5.1. Przedłożenia aktualnego zaświadczenia o niekaralności.

III.1.6. ZASADY ŚWIADCZENIA USŁUG WSPARCIA TECHNICZNEGO

1. Wykonawca zobowiązany jest zapewnić wsparcie Producenta tych urządzeń (dalej określanego jako „**Producent**”) lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta (dalej określanego jako „**Partner**”), dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt III.1.1, III.1.2, III.1.3.

2. Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, 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, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych.

III.1.7. ZASADY ŚWIADCZENIA USŁUG SZKOLENIOWYCH

1. Zamawiający wymaga dostarczenia voucherów uprawniających do przeszkolenia 4 osób z zakresu obsługi i Urządzeń NGFW. Każdy z voucherów ma uprawniać do odbycia szkolenia dla jednej osoby, niezależnie od terminu wykorzystania pozostałych voucherów.
2. Szkolenie musi być przeprowadzone w wymiarze min. 40 godzin zegarowych szkolenia, rozłożonych na 5 Dni Roboczych i obejmować:
   2.1. Podstawową i zaawansowaną administrację oraz analizę zdarzeń bezpieczeństwa zarejestrowanych przez system NGFW.
3. Szkolenie może zostać przeprowadzone w częściach, obejmujących zjazdy nie krótsze niż dwa Dni Robocze, zorganizowane w Warszawie. Zamawiający będzie uprawniony do wymagania realizacji takiego szkolenia w formie webinarium z możliwością aktywnego udziału uczestników szkolenia.
4. Dostarczone vouchery muszą mieć ważność minimum rok czasu od daty podpisania protokołu odbioru voucherów.
5. Dostarczone vouchery muszą umożliwiać realizację szkoleń w języku polskim.
6. Dostarczone vouchery maja uprawniać do odbycia szkolenia prowadzonego przez producenta przedmiotu zamówienia, (dalej określanego jako „Producent") lub autoryzowany przez Producenta podmiot.
7. Dostarczone vouchery maja uprawniać do wyboru terminu przeprowadzenia szkolenia, przypadającego nie rzadziej niż raz na pół roku kalendarzowego.

Część II – przedłużenie wsparcia systemu IPS

Przedłużenie wsparcia systemu IPS, który obecnie funkcjonuje w infrastrukturze Zamawiającego (Zamawiający do daty 20.06.2020 posiada ważne wsparcie i licencje). Zamawiający wymaga dostarczenia przedłużenia wsparcia producenta od daty zawarcia umowy na kolejne 24 miesiące na istniejące obecnie w infrastrukturze zamawiającego urządzenia IPS na zasadach opisanych poniżej.

Zamawiający przekaże informacje dotyczące aktualnie wykorzystywanej Infrastruktury IPS Zamawiającego, obejmujące producenta oraz oznaczenie rodzaju urządzeń wchodzących w skład tej infrastruktury, a także ich ilości i Serial Number, Wykonawcom, którzy złożą do Zamawiającego wniosek o udostepnienie takich informacji, zgodnie z procedurą opisana w ust. 4 pkt 4.2. Rozdziału I SIWZ, obejmującą między innymi: złożenie wniosku w formie elektronicznej, wg wzoru

przygotowanego przez Zamawiającego, złożenie oświadczenia o zachowaniu poufności wg wzoru przygotowanego przez Zamawiającego, udostępnienie przez Zamawiającego informacji poprzez wysłanie zaszyfrowanego dokumentu za pośrednictwem poczty elektronicznej oraz hasła za pośrednictwem wiadomości SMS.

III.2.1 ZASADY ŚWIADCZENIA USŁUG GWARANCJI

1. Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla Infrastruktury IPS Zamawiającego udzieloną przez Producenta tych urządzeń (dalej określanego jako „**Producent**") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**"), obejmującą okres 24 miesięcy od daty zawarcia umowy.
2. Wykonawca, zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu Gwarancji, zgodnie z następującymi zasadami:
   2.2. 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;
   2.3. Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy;
   2.4. Zgłoszone awarie będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.
3. W przypadku w którym usunięcie awarii będzie wymagać odinstalowania urządzenia, które uległo awarii:
   3.1. Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tą lokalizację;
   3.2. 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;
   3.3. Wykonawca zobowiązuje się zapewnić urządzenie zastępcze, o parametrach nie gorszych niż naprawiane urządzenie, w przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie jednego Dnia Roboczego od dnia zgłoszenia. 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.
4. Gwarant jest uprawniony do wymiany urządzenia na nowe, w przypadku w którym usunięcie awarii wymaga udostępnienia urządzenia zastępczego.

5. Wykonywania zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu gwaranta następujących wymogów:

   5.1. Przedłożenia aktualnego zaświadczenia o niekaralności.

III.2.2 Zasady świadczenia usług wsparcia technicznego

1. Wykonawca zobowiązany jest zapewnić wsparcie Producenta Infrastruktury IPS Zamawiającego (dalej określanego jako „**Producent**") lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta (dalej określanego jako „**Partner**"), dla Infrastruktury IPS Zamawiającego, przez okres 24 miesięcy od daty zawarcia umowy.
2. Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, 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, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych.

Część III – Rozbudowa infrastruktury F5 BIG-IP

Przedmiotem zamówienia jest uruchomienie funkcjonalności WAF dla urządzenia producenta F5, serii BIG-IP 5000, które Zamawiający posiada w swojej infrastrukturze.

W związku z uruchomieniem tej funkcjonalności, przedmiot zamówienia obejmuje dostawę licencji (pkt III.3.1.), świadczenie usług profesjonalnych (pkt III.3.2.) oraz realizację szkoleń dotyczących WAF (pkt III.3.3.).

III.3.1. Dostawa licencji WAF

1. W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy odpowiednie licencje konieczne do uruchomienia funkcjonalności Web Application Firewall (zwanej dalej ,,WAF") na dwóch urządzeniach F5 BIG-IP 5000, które posiada Zamawiający;
2. Zamawiający wymaga dostarczenia licencji wraz ze wsparciem producenta lub podmiotu autoryzowanego przez producenta, działającego w imieniu producenta na okres nie krótszy niż 3 lata od daty podpisania protokołu odbioru licencji, umożliwiającym korzystanie z wszystkich aktualizacji oraz baz wiedzy udostępnianych przez producenta w tym okresie;

Licencje równoważne:

3. Zamawiający dopuszcza jako „licencje równoważne" licencje zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o licencje wymienione powyżej. 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.

   Licencje równoważne (dwie sztuki) muszą zapewnić (rozszerzenie dotychczasowych funkcjonalności zawartych w dwóch obecnie znajdujących się w infrastrukturze Zamawiającego urządzeniach F5 BIG-IP 5000):

   (a) możliwość stosowania ochrony przed atakami na aplikacje internetowe i serwery WWW.

   (b) Klucze prywatne (PKI) zapisane na dysku muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

   (c) WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa musi kontrolować co najmniej:

      i. wystąpienie URL-i, długość URL-i, zabezpieczenie przed tzw.clickjackiem dla danego URL-a.
      ii. typ serwletu występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT)
      iii. przejścia pomiędzy URL-ami (servletami)
      iv. dopuszczalne metody http
      v. dopuszczalne cookie
      vi. dopuszczalne parametry w polityce
      vii. parametry dynamiczne
      viii. typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany)
      ix. oraz dopuszczalne parametry w danym serwlecie
      x. długość zapytań
      xi. nazwy hosta
      xii. wystąpień i długość parametrów (per każdy parametr)
      xiii. wystąpień i długości nagłówków
      xiv. wystąpień i długości cookies
      xv. oczekiwanych typów znaków per każdy parametr
      xvi. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku
      xvii. URL-i podatnych na CSRF

(d) Musi umożliwić profilowanie chronionej / monitorowanej aplikacji web, profilowanie musi być tworzony na podstawie analizy ruchu sieciowego.

(e) WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej.

(f) Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń).

(g) Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego. Algorytmy tworzenia profilu bezpieczeństwa WAF muszą odrzucać nadużycia w procesie nauki.

(h) Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.

(i) Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa.

(j) Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http.

(k) WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.

(l) WAF musi posiadać mechanizmy ochrony przed atakami:

a. SQL Injection
b. Cross-Site Scripting
c. Cross-Site Request Forgery
d. Session hijacking
e. Command Injection
f. Cookie/Session Poisoning
g. Parameter/Form Tampering
h. Forceful Browsing
i. Brute Force Login
j. Web Scraping
k. Cookie manipulation/poisoning
l. Dynamic Parameter tampering
m. Buffer Overflow
n. Stealth Commanding
o. Unused HTTP Methods
p. Malicious File Uploads
q. Hidden Field Manipulation.

(m) Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego musi być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.

(n) WAF musi posiadać mechanizmy ochrony przed atakami DDoS lub DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http).

(o) WAF musi blokować ataki typu Slow Loris.

(p) WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku DDoS lub DoS poprzez wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania mechanizmu browser fingerprinting, w celu wykrycia tzw. headless broser Sygnatury botów oraz wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).

(q) WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.

(r) WAF musi umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a.

(s) WAF musi umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem.

(t) WAF musi umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a.

(u) W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP.

(v) WAF musi posiadać wsparcie dla aplikacji działających w technologiach AJAX oraz JSON.

(w) WAF musi wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON.

(x) WAF musi posiadać wsparcie dla Google Web Toolkit.

(y) WAF musi posiadać możliwość ochrony komunikacji XML poprzez:

(i) - Walidację Schema/WSDL
(ii) - Wybór dozwolonych metod SOAP
(iii) - Szyfrację /deszyfrację fragmentów wiadomości SOAP
(iv) Wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie)
(v) Definiowanie możliwości użycia załączników wiadomości SOAP
(vi) Włączanie/wyłączanie podążania za odnośnikami do schematów SOAP
(vii) Walidację SOAPAction Header
(viii) Włączanie/wyłączanie możliwości użycia zewnętrznych referencji
(ix) Włączanie/wyłączanie możliwości użycia początkowych białych znaków
(x) Włączanie/wyłączanie możliwości użycia numerycznych nazw
(xi) Włączanie/wyłączanie możliwości użycia Processing Instructions

(xii) Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace

(xiii) Ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów

(xiv) Definicję dopuszczalnych znaków

(xv) Definicję sygnatur

(z) WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej muszą być dostępne w ramach tych równoważnych licencji.

(aa) WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać, co najmniej:

(bb) Directory traversal
(cc) Kodowanie typu %u
(dd) Kodowanie typu IIS backslash
(ee) IIS Unicode codepoints
(ff) Bare byte decoding
(gg) Apache whitespace
(hh) Bad unescape
(ii) Wstrzykiwanie komentarzy (np. <!-- -->)

(jj) WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolne inne ciągi znaków zdefiniowany poprzez wyrażenia regularne.

(kk) WAF musi chronić ruch przesyłany po IPv6.

III.3.2 ZASADY ŚWIADCZENIA USŁUG PROFESJONALNYCH

1. Zamawiający wymaga zapewnienia przez Wykonawcę Usług Profesjonalnych świadczonych bezpośrednio przez producenta przedmiotu zamówienia opisanego w pkt III.3.1 powyżej (dalej określanego jako „**Producent**”) lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**”) – w wymiarze łącznie 60 osobodni, przez okres 36 miesięcy od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.3.1 w pkt 2, powyżej.
2. Osoba/y realizująca Usługę Profesjonalną musi być ekspertem w obszarze związanym z F5 BIG-IP i modułem WAF oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.
3. W ramach Usług Profesjonalnych będzie m.in.:

3.1. Opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.3.1 powyżej oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Usług Profesjonalnych;

3.2. 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;

3.3. Wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.3.1 powyżej;

3.4. Konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez przedmiot zamówienia, o którym mowa w pkt III.3.1 powyżej;

3.5. Dedykowana konfiguracja modułu WAF na potrzeby chronionych aplikacji;

3.6. Tuning polityk bezpieczeństwa.

4. Osoby realizujące prace w lokalizacji Zamawiającego będą zobowiązane, na żądanie Zamawiającego, do dostarczenia aktualnego zaświadczenia o niekaralności, na min. 7 dni przed rozpoczęciem prac.
5. Zamawiający wymaga zapewnienia realizacji Usług Profesjonalnych, 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.
6. Osoby realizujące prace w lokalizacji Zamawiającego będą zobowiązane dostarczyć min. 7 dni przed rozpoczęciem prac aktualne zaświadczenia o niekaralności.

III.3.3 ZASADY ŚWIADCZENIA USŁUG SZKOLENIOWYCH

1. Zamawiający wymaga dostarczenia voucherów uprawniających do przeszkolenia 4 osób z zakresu WAF: Configuring BIG-IP ASM Application Security Manager oraz Configuring BIG-IP ASM II Application Security Manager - Advanced Workshop lub w przypadku dostarczenia licencji równoważnej opisanej powyżej, dostarczenia voucherów na szkolenie dla 6 osób w zakresie zgodnym z dostarczoną licencją równoważną.

   Każdy z voucherów ma uprawniać do odbycia szkolenia dla jednej osoby, niezależnie od terminu wykorzystania pozostałych voucherów.

2. Szkolenie musi być przeprowadzone w wymiarze min. 48 godzin zegarowych szkolenia, rozłożonych na 6 Dni Robocze i obejmować:

   2.1. Configuring BIG-IP ASM Application Security Manager 32 godziny zegarowe, 4 Dni Robocze,

2.2. Configuring BIG-IP ASM II Application Security Manager - Advanced Workshop 16 godzin zegarowych, 2 Dni Robocze

3. Szkolenie może zostać przeprowadzone w częściach wyżej wskazanych, zorganizowane w Warszawie. Zamawiający będzie uprawniony do wymagania realizacji takiego szkolenia w formie webinarium z możliwością aktywnego udziału uczestników szkolenia.
4. Dostarczone vouchery muszą mieć ważność minimum rok czasu od daty podpisania protokołu odbioru voucherów.
5. Dostarczone vouchery muszą umożliwiać realizację szkoleń w języku polskim.
6. Dostarczone vouchery maja uprawniać do odbycia szkolenia prowadzonego przez producenta Infrastruktura Zamawiającego, (dalej określanego jako „Producent") lub autoryzowany przez Producenta podmiot.
7. Dostarczone vouchery maja uprawniać do wyboru terminu przeprowadzenia szkolenia, przypadającego nie rzadziej niż raz na pół roku kalendarzowego w odniesieniu do wyżej wymienionych dwóch rodzajów szkoleń.

Część IV – rozbudowa infrastruktury DAM

Przedmiotem zamówienia jest dostawa licencji, służących do rozbudowy infrastruktury DAM Zamawiającego oraz świadczenie usług profesjonalnych dotyczących DAM zgodnie z poniższym:

III.4.1 DOSTAWA LICENCJI

Zamawiający posiada infrastrukturę DAM, dla której wymaga dostarczenia następujących licencji, wraz z subskrypcjami łącznie na okres 36 miesięcy liczonymi od dnia podpisania protokołu odbioru, zgodnie z parametrami szczegółowymi wskazanymi poniżej:

Lp.	Part number	Opis licencji	Dostawa podstawowa	Prawo opcji
1	D1E0JLL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months	6	2
2	E0L05LL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) Annual SW Subscription & Support Renewal	6	2
3	E0L05LL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) Annual SW Subscription & Support Renewal	6	2
4	D1NE3LL	IBM Security Guardium Data Protection for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months	6	2

Lp.	Part number	Opis licencji	Dostawa podstawowa	Prawo opcji
5	E0MQKLL	IBM Security Guardium Data Protection for Databases Resource Value Unit (MVS) Annual SW Subscription & Support Renewal 12 Months	6	2
6	E0MQKLL	IBM Security Guardium Data Protection for Databases Resource Value Unit (MVS) Annual SW Subscription & Support Renewal 12 Months	6	2

Zamawiający dopuszcza jako „licencje równoważne" licencje zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o licencje wymienione powyżej. 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.

Zamawiający, zobowiązuje się zakupić po sześć sztuk każdej z sześciu typów licencji opisanych powyżej jako przedmiot zamówienia, a Wykonawca zobowiązany będzie dostarczyć Zamawiającemu kolejne dwie licencje z sześciu typów po złożeniu przez Zamawiającego oświadczenia o skorzystaniu z prawa opcji – zgodnie z postanowieniami zawartymi w Istotnych Postanowieniach Umowy, stanowiących Rozdział III SIWZ.

Uszczegółowienie równoważności licencji DAM:

Ad.LP.1-3 Licencje równoważne mają umożliwić automatyczne identyfikowanie i przeszukiwanie słabych punktów zabezpieczeń i ocenę konfiguracji analizowanych Bazy Danych. W czasie weryfikacji musi umożliwić analizę używając standardów CIS (ang. Center for Internet Security) oraz STIG (ang. Security Technical Implementation Guide). Możliwe techniki weryfikacji musza być regularnie aktualizowane za pośrednictwem Producenta. Licencja również musi:

- umożliwić wykonania testów bezpieczeństwa, które nie mogą zakłócić dostępność i działanie systemu analizowanego. Po testach musi udostępniać informacje o wykrytych słabych punktach co najmniej w postaci identyfikatorów CVE.

- musi umożliwić pokazanie jak historycznie zmieniają się podatności w czasie.

- umożliwić weryfikacje i testy j.w. w systemach bazodanowych opartych o technologie Oracle, MSSQL. MySQL, MariaDB, MongoDB, DB2, PostgreSQL.

- umożliwić użycie ich za pomocą zaimplementowanego w infrastrukturze (Zamawiającego) systemu IBM GUARDIUM (w konsoli zarządzającej).

Ad.LP.4-6 Licencje równoważne mają umożliwić systemowi IBM GUARDIUM zaimplementowanemu w infrastrukturze (Zamawiającego) na powiększenie ilości monitorowanych Baz danych, które są uruchomione na 8 serwerach fizycznych. Licencja również musi:

- umożliwić monitoring i ochronę Baz danych pod katem bezpieczeństwa (operacje SQL w czasie rzeczywistym) w systemach bazodanowych opartych o technologie: Oracle, MSSQL. MySQL, MariaDB, MongoDB, DB2, PostgreSQL zainstalowanych na systemach operacyjnych: Linux, Unix, Solaris, AIX, Windows.

- reguły bezpieczeństwa mogą być tworzone w oparciu o wskazane wartości występujące w zapytaniu SQL, czasie wystąpienia, na podstawie adresacji IP źródła i celu oraz ważności zidentyfikowanych informacji w bazie danych.

- umożliwić identyfikację czy w bazach danych są informacje jak: dane osobowe (w tym PESEL) i inne dane opisane w oparciu o wyrażenia regularne.

- umożliwić monitoring czy Zamawiający jest zgodny z GDPR, HIPAA, SOX, PCI w kontekście dostępów do danych zawartych w chronionych bazach danych.

- umożliwić reakcje (systemu DAM) jak monitorowanie, alertowanie, blokowanie i maskowanie informacji w przypadku wykrycia incydentu lub zdarzenie bezpieczeństwa zgodnie z zastosowaną regułą bezpieczeństwa.

III.4.2 ZASADY ŚWIADCZENIA USŁUG PROFESJONALNYCH:

1. Zamawiający wymaga zapewnienia przez Wykonawcę Usług Profesjonalnych świadczonych bezpośrednio przez producenta przedmiotu zamówienia opisanego w pkt III.4.1 powyżej (dalej określanego jako „**Producent**") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**") – w wymiarze łącznie 60 osobodni, przez okres 36 miesięcy od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.4.1, powyżej.
2. Osoba/y realizująca Usługę Profesjonalną musi być ekspertem w obszarze związanym z DAM oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.
3. W ramach Usług Profesjonalnych będzie m.in.:
   3.1. Opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.4.1 powyżej oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Usług Profesjonalnych;
   3.2. 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;

3.3. Wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.4.1 powyżej;

3.4. Konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez przedmiot zamówienia, o którym mowa w pkt III.4.1, powyżej;

3.5. Dedykowana konfiguracja DAM na potrzeby chronionych baz danych;

3.6. Tuning polityk bezpieczeństwa, konfiguracja polityk DAM na potrzeby chronionych baz danych;

3.7. Wsparcie w analizie wyników pracy systemu DAM;

3.8. Wsparcie w konfiguracji środowiska bazodanowego na potrzeby DAM.

4. Zamawiający wymaga zapewnienia realizacji Usług Profesjonalnych, 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.

Część V – dostawa stacji roboczych i monitorów

1. Wykonawca, na co najmniej 1 Dzień Roboczy przed dostawą, jest zobowiązany do przekazania Zamawiającemu na adres e-mail wskazany przez Zamawiającego w Umowie zestawienia w formacie .csv wszystkich dostarczonych urządzeń, zgodnie ze złożoną Ofertą, zawierającego takie informacje jak: producent, typ, model, numer seryjny, okres obowiązywania gwarancji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego, cenę jednostkową netto, cenę jednostkową brutto, MAC adres karty sieciowej, numer seryjny dysku (jeśli dotyczą).
2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. Dostarczany Sprzęt musi być kompletny, tj.: mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
4. Zamawiający nie dopuszcza sprzętu prefabrykowanego, wymagana jest dostawa sprzętu fabrycznie nowego, nieużywanego.
5. Zamawiający może wykonywać uprawnienia z tytułu rękojmi niezależnie od uprawnień wynikających z gwarancji jakości.
6. Wykonawca zobowiązuje się w ramach realizacji przedmiotu zamówienia do dostarczenia Zamawiającemu sprzętu opisanego w OPZ, w terminie maksymalnie 30 Dni Roboczych od daty zawarcia umowy.
7. Sprzęt zostanie dostarczony do siedziby Centralnego Ośrodka Informatyki, mieszczącego się przy ul. Aleje Jerozolimskie 132-136, 02-305 Warszawa; budynek Delta, środkiem transportu, którego waga nie przekracza 6 ton.

III.5.1 Specyfikacja Stacji Roboczej

Specyfikacja Stacji Roboczej wraz z niezbędnym wyposażeniem – 3 szt.	
Produkt	Stacja robocza klasy PC.
Zestaw	1. Stacja robocza. 2. Klawiatura USB w układzie polski programisty. 3. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll).
Obudowa	1. Typu Tower z zasilaczem i przewodem zasilającym; 2. Kolor: czarny, szary lub srebrny.
Procesor	Rodziny x 86, który posiada 8 logicznych rdzeni i jest w stanie zapewnić wydajność procesora na poziomie co najmniej 12377* punktów Passmark CPU Mark, wg zestawienia dla systemów jednoprocesorowych publikowanego przez producenta testu opublikowanego na dzień otwarcia ofert, który dostępny jest na stronie: www.cpubenchmark.net/cpu_list.php.
Pamięć operacyjna RAM	Min. 32 GB – DDR4 ECC. Minimum 4 wolnych banków pamięci na potrzeby przyszłej rozbudowy.
Parametry pamięci masowej	Min. 1 szt. dysk minimum 1 TB 7200 obr./min. plus 1 dysk SSD minimum 250GB z interfejsem PCIe.
Karta graficzna	Umożliwiająca podłączenie minimum 2 monitorów kompatybilna z monitorem wskazanym w niniejszej części dokumentu.
Karta dźwiękowa	Zintegrowana.
Napęd DVD+/-RW	Nie wymagany
System operacyjny	Nie wymagany
Standardy i certyfikaty	Deklaracja zgodności CE dla oferowanego modelu (załączyć przy dostawie).
Złącza	1. Do podłączenia monitora wskazanego w niniejszej części dokumentu – minimum 2 szt.; 2. Porty USB 3.1 – minimum 2 szt. z przodu obudowy. 3. Porty USB 3.0 – minimum 4 szt. z tyłu obudowy. 4. RJ-45 – 1 szt. (karta sieciowa zintegrowana 1 Gb/s). 5. Zasilanie (AC) – 1 szt.
Zasilanie	Wewnętrzny zasilacz 750 W, sprawność min. 90%, aktywny stabilizator PFC.
BIOS	BIOS w standardzie UEFI musi posiadać następujące cechy: 1. BIOS musi zawierać nieulotną informację z nazwą producenta, nazwą produktu, jego numerem seryjnym, wersji BIOS, a także informację o

Specyfikacja Stacji Roboczej wraz z niezbędnym wyposażeniem – 3 szt.	
	typie zainstalowanego procesora, ilości i typie pamięci RAM, rodzaju układu graficznego. 2. Informacji o dysku twardym: model oraz pojemność. 3. Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, portów USB z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego, urządzeń zewnętrznych. 4. Funkcja blokowania/odblokowania gotowania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość – bez potrzeby uruchamiania systemu operacyjnego z dysku twardego stacji roboczej lub innych, podłączonych do niego urządzeń zewnętrznych – ustawienia hasła na poziomie administratora.
Bezpieczeństwo	BIOS musi posiadać możliwość: 1. Skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS. 2. Możliwość ustawienia hasła na dysku (drive lock). 3. Blokady/wyłączenia portów USB, COM, karty sieciowej. 4. Kontroli sekwencji boot-ującej. 5. Startu systemu z urządzenia USB. 6. Funkcja blokowania boot-owania stacji roboczej z zewnętrznych urządzeń. 7. Blokowania zapisu na dyskach wymiennych USB. Stacja robocza musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (min. TPM 2.0).
Klawiatura	1. Układ QWERTY. 2. Kolor czarny. 3. Interfejs: USB. 4. Blok numeryczny.
Mysz	Mysz przewodowa, optyczna, ze złączem USB, z min. dwoma przyciskami oraz rolką (scroll).

III.5.2 SPECYFIKACJA MONITORÓW.

Każdy dostarczony Monitor liczony jest jako zestaw, w skład którego wchodzi Monitor oraz niezbędne wyposażenie dodatkowe tj.:

Specyfikacja Monitora wraz z niezbędnym wyposażeniem dodatkowym – 7 szt.	
Produkt	Monitor
Wyposażenie dodatkowe	1. Monitor; 2. Podstawa Monitora. 3. Przewód zasilający min. 1,5m. 4. Przewód DisplayPort męski-męski min. 1,5m. 5. Przewód HDMI męski-męski min. 1,5m. 6. Przewód USB-C umożliwiający połączenie Monitora z stacją roboczą min. 1,5m.
Matryca	1. Matowa. 2. Podświetlenie matrycy LED. 3. Matryca obsługująca natywnie rozdzielczość 2560x1440. 4. Częstotliwość odświeżana min 144 Hz. 5. Przekątna min 27”. 6. Proporcje 16x9 lub 16x10. 7. Kąty widzenia: • Poziom: 178 stopni. • Pion: 178 stopni. 8. Jasność 350 cd/m2. 9. Kontrast 1000:1.
Interfejsy	1. Wejście HDMI min. 1.4 x 1. 2. Wejście DisplayPort min. 1.2 x1; 3. Wejście USB min. 2.0 typ A x2;
Funkcje ogólne	1. Technologia redukcji migotania; 2. Tryb ochrony oczu przed nadmiernym niebieskim światłem; 3. Język menu OSD polski lub angielski.
Cechy fizyczne	1. Regulacja wysokości w zakresie wysokości od min. 50 mm. do min. 130mm licząc odległość od dolnej krawędzi Monitora od powierzchni, na której stoi Monitor. 2. Obrotowy ekran (PIVOT) w zakresie min. 0-90 stopni. 3. Regulacja pochylenia (TILT) w zakresie min. -5-20 stopni. 4. Zgodny ze standardem VESA. 5. Kolor obudowy czarny, odcienie szarości lub srebrny. 6. Zasilacz wbudowany w bryłę Monitora.
Zarządzanie energią	1. Pobór mocy podczas spoczynku (standby) max 0,5W. 2. Klasa energetyczna min. B.

III.5.3 WYMAGANIA GWARANCYJNE DLA STACJI ROBOCZYCH I MONITORÓW

1.1. Przedmiotem zamówienia jest jednorazowa dostawa stacji roboczych i monitorów, zgodnie z specyfikacją wymienioną w OPZ i gwarancją producenta na okres minimum 36 miesięcy.

1.2. Dostarczony Sprzęt musi być objęty minimum 36 miesięczną gwarancją producenta, realizowaną w zakresie serwisu gwarancyjnego przez producenta lub autoryzowanego partnera serwisowego producenta..

1.3. Zasady świadczenia gwarancji dla Sprzętu:

1) Usunięcie awarii – do 3 Dni Roboczych od dnia zgłoszenia (przyjmowanie zgłoszeń w Dni Robocze w godzinach 8.00 — 16.00 telefonicznie, faksem lub e-mailem),
2) w razie nieusunięcia awarii Sprzętu w terminach, o których mowa powyżej Wykonawca dostarczy na czas naprawy urządzenie zastępcze, o parametrach technicznych nie gorszych od parametrów technicznych sprzętu naprawianego (zastosowanie obejścia) z zastrzeżeniem, że Zamawiający zatrzyma dysk twardy z takiego urządzenia;
3) Zamawiający zastrzega sobie prawo do samodzielnego demontażu/montażu dysku bez utraty gwarancji producenta;
4) w przypadku stwierdzenia uszkodzenia nośnika danych (np. dysku twardego, dysku SSD), należy wymienić go na nowy, wolny od wad, o tych samych lub lepszych parametrach, bez zwrotu uszkodzonego dysku twardego / SSD;
5) w przypadku braku możliwości naprawy Sprzętu w wymaganym terminie (w miejsce Sprzętu, który nie może być przez Wykonawcę naprawiony), w ramach realizacji zobowiązań wynikających z Umowy, Wykonawca zobowiązany jest do dostarczenia do lokalizacji, o której mowa w Części V – dostawa stacji roboczych i monitorów w pkt 7 i przekazania Zamawiającemu (bez dodatkowego wynagrodzenia) innego Sprzętu, o parametrach technicznych nie gorszych od parametrów Sprzętu uszkodzonego, a następnie świadczenia gwarancji i wsparcia technicznego w stosunku do tego Sprzętu przez okres obowiązywania Umowy;
6) gwarancja musi być świadczona przez serwis producenta Sprzętu lub przez autoryzowanego partnera serwisowego producenta Sprzętu - przez pracowników producenta urządzeń lub przez pracowników partnera producenta, dysponujących odpowiednimi uprawnieniami i kwalifikacjami, potwierdzonymi certyfikatami wystawionymi przed producenta urządzeń, które Wykonawca dostarczy wraz z dostawą sprzętu.