Dnia 04.07.2018 r.

Szacowanie wartości zamówienia nr 01/07/2018/Z004/BP/SZ

Zamawiający w związku z zamiarem ogłoszenia procedury zasady konkurencyjności przeprowadza procedurę szacowania zamówienia zgodnie z Wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014 – 2020.

W związku z powyższym, Zamawiający zwraca się z prośbą o oszacowanie wartości zamówienia opisanego w pkt 2 poniżej.

Niniejsza prośba nie stanowi procedury zasady konkurencyjności, a odpowiedź uzyskana przez Zamawiającego w procedurze szacowania nie będzie przez Zamawiającego traktowana jako oferta.

1. **Zamawiający**

Wyższa Szkoła Bankowa we Wrocławiu, ul. Fabryczna 29-31; 53-609 Wrocław, wpisana do Rejestru Uczelni Niepublicznych i Związków Uczelni Niepublicznych pod numerem 146,

1. **Opis przedmiotu zamówienia**
   1. **Cel zamówienia**

Celem Przedmiotem zamówienia jest wyłonienie Wykonawcy na dostawę, wdrożenie, konfigurację i wsparcie techniczne oprogramowania Sophos XG FullGuard Plus lub programu równoważnego

Zamówienie będzie realizowane w ramach projektu współfinansowanego Europejskiego Funduszu Społecznego: INFORMATYZACJA, UMIĘDZYNARODOWIENIE, PRAKTYCZNOŚĆ - filary Zintegrowanego Programu Uczelni w Wyższej Szkole Bankowej we Wrocławiu, POWR.03.05.00-00-Z004/17.

* 1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest oprogramowanie Sophos XG FullGuard Plus (licencja edukacyjna 4 lata) lub programu równoważnego dla potrzeb Wyższej Szkoły Bankowej we Wrocławiu.

1. Charakterystyka zamawianego oprogramowania

Typ systemu ochrony:

1. System ochrony sieci musi być dostarczony w postaci komercyjnej platformy z zabezpieczonym systemem operacyjnym jako licencja do instalacji na sprzęcie zamawiającego lub środowisku VM (virtual applinace).

2. Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).

3. Wymagania systemowe:

System ochrony musi spełniać wymagania w niżej wymienionym zakresie.

- Musi istnieć możliwość instalacji na fizycznym sprzęcie zgodny z x86

- Musi istnieć możliwość instalacji jako VM (Virtual Machine) w środowisku VMware, Citrix, Hyper-V lub KVM.

- Nielimitowana ilość użytkowników

- Licencja do instalacji na zasobie (sprzętowym lub wirtualnym) posiadającym 8 rdzeni procesora i 16GB pamięci RAM.

- Nielimitowana (sztucznie ograniczana) liczba użytkowników i interfejsów sieciowych

- Licencja musi umożliwiać aktywację i użytkowanie wszystkich opcjonalnych modułów funkcjonalnych przez okres 4 lat.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY

Zarządzanie i utrzymanie:

1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne takie jak: ping, traceroute, name lookup, route lookup. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.

2. Rozwiązanie musi oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.

3. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

4. System musi oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.

5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.

6. System musi oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady musi być swobodnie definiowane przez administratora.

7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host,

harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów musi być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.

8. System musi oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.

9. Rozwiązanie musi zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.

10. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.

11. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3.

12. System musi zapewniać monitorowanie w czasie rzeczywistym stanu systemu (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych).

13. System musi oferować możliwość integracji z centralnym systemem do zarządzania.

14. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub via email.

15. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.

16. Rozwiązanie musi zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.

17. Zarządzanie licencjami i subskrypcjami musi odbywać się za pośrednictwem portalu on-cloud

18. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).

19. System ochrony musi umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.

20. W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie).

Zapora sieciowa, konfiguracja sieciowa oraz routing:

1. Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.

2. Rozwiązanie musi umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.

3. System musi umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.

4. Polisy zapory muszą umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.

5. Rozwiązanie musi zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.

6. System ochrony musi zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.

7. Rozwiązanie musi oferować możliwość definiowania własnych stref zapory sieciowej.

8. Rozwiązanie musi pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.

9. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).

10. System musi zapewniać ochrona przed skanowaniem portów (portscan blocking).

11. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).

12. Rozwiązanie musi zapewniać obsługę routingu statycznego.

13. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).

14. System musi oferować wsparcie dla IGMP snooping.

15. Rozwiązanie musi zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy

(upstream/parrent proxy).

16. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.

17. System musi oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.

18. System musi oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.

19. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.

20. Rozwiązanie musi umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.

21. Rozwiązanie musi oferować wsparcie dla Policy Based Routing oraz Multipath Rules.

23. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).

24. System musi zapewniać pełną obsługę usług DNS, DHCP oraz NTP.

25. System musi oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.

26. Rozwiązanie musi zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).

Podstawowe kształtowanie pasma oraz limity ilości danych:

1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.

2. Rozwiązanie musi pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.

3. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.

Bezpieczna sieć bezprzewodowa:

1. System musi zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.

2. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater.

3. Wdrożenie punktów dostępowych sieci bezprzewodowej musi odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe muszą automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.

4. Zarządzanie punktami dostępowymi sieci bezprzewodowej musi odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.

5. Punkty dostępowe sieci bezprzewodowej muszą być powiązane z siecią lokalną, siecią VLAN lub

dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej.

6. Rozwiązanie musi umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania

identyfikatorów sieci bezprzewodowej.

7. Rozwiązanie musi oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.

8. Rozwiązanie musi zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).

9. Rozwiązanie musi oferować wsparcie dla IEEE 802.11r (Fast Transition).

10. System musi umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.

11. Dostęp do sieci bezprzewodowej musi być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.

12. System musi zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden.

13. System musi pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe.

14. Rozwiązanie musi zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych.

Autoryzacja użytkowników:

1. Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.

2. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.

3. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+.

4. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.

5. System musi umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password).

6. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.

7. System musi oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.

8. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.

9. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.

Samoobsługowy portal dla użytkowników:

1. Rozwiązanie musi udostępniać plik instalacyjny agenta do autentykacji w sieci.

2. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).

3. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.

4. Rozwiązanie musi udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów

operacyjnych w tym dla Mac OS X, Linux, iOS, Android.

5. Rozwiązanie musi umożliwiać zmianę nazwy użytkownika oraz hasła.

6. Rozwiązanie musi pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.

7. Rozwiązanie musi oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.

Podstawowe opcje VPN (wymagania obowiązkowe):

1. System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:

- Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub

współdzielonego klucza Pre-Shared Key (PSK),

- Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu

samoobsługowego portalu użytkownika).

Klient IPSec VPN (dostępny osobno, wymagania obowiązkowe):

1. Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.

2. Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.

3. Wsparcie dla split-tunneling.

4. Wsparcie dla NAT-traversal.

5. Monitorowanie stanu połączenia.

OCHRONA SIECI (wymagania obowiązkowe):

IPS:

1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 7000 sygnatur. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. System musi generować alerty w przypadku wykrycia ataku.

ATP:

1. System ochrony musi zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.

Synchronizacja z endpoint:

2. System musi mieć możliwość rozbudowy uruchomienia synchronizacji stanu bezpieczeństwa

komputerów w sieci LAN z Firewallem. Możliwość automatycznego odcięcia komputera/ów zainfekowanych. (wymagane dodatkowe oprogramowanie nie będące częścią tego postępowania).

Clientless VPN:

1. Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.

OCHRONA I KONTORLA WEB ORAZ APLIKACJI

Ochrona i kontrola Web:

1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.

2. Moduł musi pozwalać na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).

3. System musi oferować inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.

4. System musi oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.

5. Rozwiązanie musi automatyczne odpytywać bazy producenta w trybie rzeczywistym.

6. Rozwiązanie musi zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).

7. Rozwiązanie musi oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją

certyfikatów.

8. System musi oferować funkcję Web cache dla ograniczenia zużycia pasma.

9. System musi filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.

10. Rozwiązanie musi zapewniać filtrowanie plików Activex, apletów , cookies.

11. System musi zapewniać możliwość emulacji skryptów JavaScript.

12. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

13. Rozwiązanie musi zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.

14. Rozwiązanie musi zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.

15. Rozwiązanie musi umożliwiać blokadę stron HTTPS.

16. Rozwiązanie musi blokować anonimowe proxy działające poprzez HTTP i HTTPS.

17. Rozwiązanie musi umożliwiać definiowanie polityk dostępu do Internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.

18. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo organizacji.

Ochrona i kontrola aplikacji:

1. Rozwiązanie musi oferować bazę danych opisująca, co najmniej 2 500 aplikacji.

2. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.

3. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikro-aplikacji.

4. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu,

szyfrowania.

5. Rozwiązanie musi umożliwiać blokowanie:

- aplikacji, które pozwalają na transfer plików (np. P2P).

- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.

- proxy uruchamianych poprzez przeglądarki internetowe.

- streaming media (radio internetowe, Youtube, Vimeo).

6. Rozwiązanie musi umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.

Kształtowanie pasma dla Web i Aplikacji:

1. Rozwiązanie musi oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku

upload/download/łącznie.

2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.

3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym oraz

współdzielonym.

OCHRONA I KONTROLA EMAIL

Ochrona i kontrola Email:

1. Rozwiązanie musi oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Mail Transfer Agent.

2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS.

3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.

4. System musi umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.

5. Rozwiązanie musi automatyczne odpytywać bazy producenta w trybie rzeczywistym.

6. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.

7. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.

8. Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.

9. System musi wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści

wiadomości.

10. Rozwiązanie musi oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora.

11. System musi oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP oraz IMAP.

12. Rozwiązanie musi umożliwiać dodanie stopki do każdej wiadomości wychodzącej.

13. Rozwiązanie musi umożliwiać archiwizowanie wiadomości email.

14. Rozwiązanie musi współpracować, z co najmniej dwoma bazami RBL.

15. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów IP i email.

16. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.

17. Rozwiązanie musi blokować spam w postaci plików graficznych np. wiadomości z tekstem osadzonym w obrazku.

Kwarantanna Email:

1. System musi zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako spam z opcją powiadamiania użytkownika.

2. System musi zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.

3. Rozwiązanie musi zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania po dacie, nadawcy, odbiorcy, temacie wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika).

OCHRONA SERWERÓW APLIKACYJNYCH WEB (wymagania obowiązkowe)

WAF:

1. Dodatkowy moduł ochrony klasy Web Application Firewall.

2. Funkcjonalność oparta o mechanizm Reverse Proxy.

3. Rozwiązanie musi oferować mechanizm URL hardening with deep-linking and directory traversal prevention.

4. Rozwiązanie musi oferować mechanizm Form hardening.

5. Rozwiązanie musi oferować ochronę przed SQL injection.

6. Rozwiązanie musi oferować ochronę przed Cross-site scripting.

7. System musi zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL).

8. System musi umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.

9. System musi pozwalać na podpisywanie plików cookies.

10. Rozwiązanie musi oferować wsparcie dla Path-based routing.

11. Rozwiązanie musi oferować wsparcie dla Outlook Anywhere.

12. Rozwiązanie musi oferować mechanizm Reverse authentication z automatycznym dodawaniem prefixu lub suffixu w trakcie autoryzacji użytkownika.

13. Rozwiązanie musi umożliwiać publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych.

14. Rozwiązanie musi oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing).

15. System musi umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych.

16. System musi umożliwiać stosowanie operatorów logicznych AND/OR.

OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY

On-cloud Sandboxing:

1. Rozwiązanie musi posiadać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox umożliwiający dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll.

2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.

3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.

4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym: .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.

5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS.

6. Rozwiązanie musi zawierać system ochrony ze średnim realnym czasem analizy kodu poniżej 120 sekund.

7. System musi oferować szczegółowe raporty wyników analizy.

LOGOWANIE I RAPORTOWANIE

1. System musi umożliwiać składowanie oraz archiwizację logów.

2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.

3. System musi zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.

4. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.

5. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).

6. Rozwiązanie musi umożliwiać wysyłanie raportów via email.

7. Rozwiązanie musi generować raporty w PDF, HTML i XLS.

8. Rozwiązanie musi oferować możliwość wysyłania logów systemowych, do co najmniej 3 serwerów syslog.

9. System musi zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.

10. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.

11. Rozwiązanie musi oferować możliwość zanonimizowania danych w raportach.

12. System musi umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.

13. System musi pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.

1. Pozostałe.

Wsparcie techniczne do oprogramowania musi być prowadzone przez producenta w trybie 24 godziny przez 7 dni w tygodniu, na okres 4 lat. W ramach wsparcia technicznego producent zobowiązany jest do dostarczania aktualizacji i poprawek oprogramowania dla wszystkich dostarczonych modułów.

* 1. **Zasady ustalania wynagrodzenia za wykonanie przedmiotu zamówienia**

Wynagrodzenie obejmuje wszystkie elementy składowe Szacowania wartości zamówienia, płatne jednorazowo po podpisaniu protokołu odbioru.

* 1. **Miejsce dostawy przedmiotu zamówienia oraz wykonania pozostałych usług**

**Wyższa Wyższa Szkoła Bankowa we Wrocławiu,** ul. Fabryczna 29-31; 53-609 Wrocław; budynek B, osoba do kontaktu: Marcin Pieleszek, marcin.pieleszek@gmail.com

* 1. **Kod CPV:**

Kod CPV: **48000000-8 – Pakiety oprogramowania i systemy informatyczne**

* 1. **Dodatkowe przedmioty zamówienia**

Zamawiający nie przewiduje dodatkowych przedmiotów zamówienia.

* 1. **Zamówienia uzupełniające**

Zamawiający nie przewiduje zamówień uzupełniających.

1. **Terminy realizacji zamówienia**

Harmonogram realizacji zamówienia:

1. Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia w terminie do 24.08.2018 r.

2. Za termin wykonania przedmiotu zamówienia uważa się jego dostarczenie do siedziby Zamawiającego oraz uruchomienie i skonfigurowanie oprogramowania w ramach posiadanej przez Zamawiającego infrastruktury.

3. Wsparcie techniczne opisane w punkcie 2.2. Szacowania wartości zamówienia, będzie obejmowało czteroletni okres trwania licencji na zakupione oprogramowanie.

1. **Warunki udziału w postępowaniu**

**Uprawnienia do wykonania określonej działalności lub czynności**

W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają niżej wymienione warunki udziału w postępowaniu.

* 1. **Sytuacja ekonomiczna i finansowa**

Wykonawca znajduje się w sytuacji ekonomicznej i finansowej zapewniającej terminowe wykonanie przedmiotu zamówienia.

Wykonawca nie znajdują się w stanie likwidacji ani nie jego ogłoszono upadłości.

Wykonawca nie zalega z uiszczeniem podatków, opłat oraz składek na ubezpieczenia

społeczne i zdrowotne.

* 1. **Dodatkowe warunki:**

Wykonawca przestawi pisemne referencje od klienta, u którego została wykonana instalacja i konfiguracja narzędzia o parametrach technicznych i funkcjonalnych wskazanych w Szacowaniu wartości zamówienia oraz zadeklaruje możliwość organizacji wizyty (lub telekonferencji) referencyjnej u klienta który wystawił referencje.

1. **Sposób dokonania oceny spełnienia warunków udziału w postępowaniu**

Ocena spełnienia warunków udziału w postępowaniu przeprowadzona zostanie w oparciu o podpisane przez Wykonawcę oświadczenie o spełnieniu wymagań Zamawiającego określonych w załączniku nr 1 do Szacowania wartości zamówienia oraz dokumentów wymienionych w pkt. 7.

1. **Wykluczenia z udziału w postępowaniu**

W celu uniknięcia konfliktu interesów, zamówienie nie może być udzielane podmiotom powiązanym osobowo lub kapitałowo z Zamawiającym tj. Wyższą Szkołą Bankową we Wrocławiu. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym tj. Wyższą Szkołą Bankową we Wrocławiu lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego tj. Wyższej Szkoły Bankowej we Wrocławiu lub osobami wykonującymi w imieniu Zamawiającego tj. Wyższej Szkoły Bankowej we Wrocławiu czynności związanych z przeprowadzeniem procedury wyboru Wykonawcy, a Wykonawcą. Przez powiązania kapitałowe lub osobowe rozumie się w szczególności:

* + uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
  + posiadanie co najmniej 10% udziałów lub akcji,
  + pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
  + pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Potwierdzeniem spełnienia ww. warunku będzie złożenie przez Wykonawcę Oświadczenia o braku powiązań stanowiącego załącznik nr 2 do niniejszego Szacowania wartości zamówienia.

1. **Lista Dokumentów wymaganych od Wykonawcy**

Lista Dokumentów, które Wykonawca zobowiązany jest złożyć w odpowiedzi na Szacowanie wartości zamówienia:

1. Załącznik nr 1  do Szacowania wartości zamówienia nr 01/07/2018/Z004/BP/SZ - Formularz **szacowania wartości zamówienia** – wypełniony i podpisany przez Wykonawcę lub osobę/osoby upoważnione do reprezentacji Wykonawcy.
2. Załącznik nr 2 do Szacowania wartości zamówienia nr 01/07/2018/Z004/BP/SZ – Oświadczenie o braku wzajemnych powiązań kapitałowych lub osobowych Wykonawcy i Zamawiającego - wypełniony i podpisany przez Wykonawcę lub osobę/osoby upoważnione do reprezentacji Wykonawcy.
3. Dokumenty potwierdzające uprawnienia osób do podpisania oferty, jeżeli nie wynika to z dokumentów rejestrowych.
4. **Sposób przygotowania i składania ofert**

Wykonawca może złożyć tylko jeden Formularz szacowania wartości zamówienia wypełniony w języku polskim w postaci dokumentów wskazanych w punkcie 7. Szacowania wartości zamówienia.

Dokumenty wskazane w punkcie 7. Szacowania wartości zamówienia (Formularz szacowania wartości zamówienia wraz z załącznikami) należy wysłać mailem na adres:

bartlomiej.piskor@wsb.wroclaw.pl do dnia **10.07.2018 roku do godziny 10:00**.

PROSI SIĘ O WYSYŁANIE WIADOMOŚCI O WIELKOŚCI MAKSYMALNIE 10MB. W PRZYPADKU PRZEKROCZENIA TEJ WIELKOŚCI NALEŻY WYSYŁAĆ WIADOMOŚCI W DWÓCH LUB W TRZECH E-MAILACH.

Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem Formularza szacowania wartości zamówienia. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu. Formularz szacowania wartości zamówienia zatrzymuje Zamawiający.

1. **Załączniki do Szacowania wartości zamówienia:**

* Załącznik nr 1 do Szacowania wartości zamówienia nr **01/07/2018/Z004/BP/SZ** - **Formularz szacowania wartości zamówienia**.
* Załącznik nr 2 do Szacowania wartości zamówienia nr **01/07/2018/Z004/BP/SZ** -[**Oświadczenie o braku wzajemnych powiązań kapitałowych lub osobowych Wykonawcy i Zamawiającego.**](https://www.wsb.pl/wroclaw/sites/wsb.pl.wroclaw/files/default_images/zalacznik_nr_2_-_oswiadczenie_o_braku_powiazan_do_szacowania_2.doc)