Piątnica, 20.12.2024 r.

**Zapytanie ofertowe nr 10/2024**

W związku z realizacją projektu:

pt.: „Automatyzacja, robotyzacja i cyfryzacja procesów produkcyjnych i organizacyjnych w celu wzrostu innowacyjności i produktywności OSM Piątnica, przy zachowaniu bezpieczeństwa danych i pozytywnym wpływie na środowisko naturalne”

w ramach naboru nr KPOD.01.11-IP.06-002/23 tytuł Inwestycje wspierające robotyzację i cyfryzację   
w przedsiębiorstwach (A2.1.1) organizowanego przez Ministerstwo Aktywów Państwowych

ogłaszamy postępowanie ofertowe na wybór wykonawcy systemu do zapewnienia bezpieczeństwa danych :

1. ***Opis przedmiotu zamówienia (specyfikacja):***
   1. Zamawiający wymaga dostarczenia dwóch typów urządzeń UTM opisanych w tym dokumencie odpowiednio jaki Firewall TYP 1 oraz Firewall TYP 2:
      1. Zamawiający wymaga dostarczenia dwóch urządzeń Firewall typ 1 (szczegółowe wymagania funkcjonalne w punkcie 2.11)
      2. Zamawiający wymaga dostarczenia dwóch urządzeń Firewall typ 2 (szczegółowe wymagania funkcjonalne w punkcie 2.12)
   2. Zamawiający wymaga, aby wszystkie komponenty programowe oraz urządzenia wchodzące w skład systemu bezpieczeństwa pochodziły od jednego producenta.
   3. Zamawiający wymaga, aby wszystkie komponenty systemu bezpieczeństwa zainstalowane zostały lokalnie w ramach infrastruktury Zamawiającego.
   4. Zamawiający wymaga, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta.
   5. Zamawiający wymaga, aby dostarczone urządzenia były nowe oraz pochodziły z bieżącej produkcji. Zamawiający nie dopuszcza dostawy urządzeń, które mogły być używane w innych projektach i zostały poddane procesowi odnowienia.
   6. Zamawiający zobowiązuje Wykonawcę do potwierdzenia, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Wykonawca nie może zaoferować sprzętu i oprogramowania, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
   7. Zamawiający wymaga, aby dostarczony system zabezpieczeń był produktem o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej 36 miesięcy z rzędu.
   8. Zamawiający wymaga, aby wszystkie określone w niniejszym dokumencie funkcje systemu były realizowane w aktualnie dostępnych komercyjnie urządzeniach oraz wersjach oprogramowania.
   9. Zamawiający wymaga aby elementy systemu zostały dostarczone ze stabilną wersją oprogramowania. Oznacza to, iż rozwiązanie (urządzenia + oprogramowanie) musi być dostępne na rynku nie krócej niż 3 miesiące od daty ogłoszenia postępowania przetargowego.
   10. System bezpieczeństwa musi zostać dostarczony z zestawem licencji pozwalających na realizację następujących funkcjonalności przez okres 3 lat:

* funkcja firewall
* wykrywanie i przeciwdziałanie próbom włamań (IPS)
* tworzenie reguł polityki bezpieczeństwa z wykorzystaniem definicji konkretnych aplikacji (kontrola aplikacji)
* tworzenie reguł polityki bezpieczeństwa z wykorzystaniem kategorii URL
* ochrona antywirusowa
* wykrywanie i blokowanie komunikacji z sieciami botnet
* tworzenie reguł polityki w oparciu o tożsamość użytkownika (możliwość korelacji tożsamości użytkowników z wykorzystywanym adresem IP)
* wykonywanie inspekcji ruchu szyfrowanego
* możliwość realizacji połączeń IPSec VPN
* możliwość ochrony przed atakami typu 0-day

1. ***Zapory sieciowe (specyfikacja)***
   1. Ogólne (redundancja / tryby pracy)
      1. Urządzenia Firewall TYP 1 muszą posiadać możliwość pracy w klastrze w trybie Active-Standby lub Active-Active. Mechanizm klastrowania musi zapewniać funkcję synchronizacji informacji o stanie połączeń sieciowych pomiędzy urządzeniami wchodzącymi w skład klastra.
      2. Mechanizm klastrowania w ramach urządzeń Firewall TYP 1 musi obsługiwać do 5 urządzeń UTM.
      3. Urządzenia Firewall TYP 2 muszą posiadać możliwość pracy w klastrze w trybie Active-Standby i obsługiwać minimum 2 urządzenia UTM. Mechanizm klastrowania musi zapewniać funkcję synchronizacji informacji o stanie połączeń sieciowych pomiędzy urządzeniami wchodzącymi w skład klastra.
      4. Interfejsy zapory sieciowej muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI),w trybie transparentnym oraz w trybie pasywnego nasłuchu (monitoring).
      5. Tryb pracy interfejsu zapory sieciowej musi być ustalany w konfiguracji interfejsu sieciowego, a zapora musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
      6. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 1024 znaczników VLAN w trybie Gateway oraz 4096 znaczników w trybie wirtualnych systemów.
      7. Urządzenia UTM muszą obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP, OSPF (v2 oraz v3)
      8. Zapora sieciowa musi posiadać możliwość pracy w trybie serwera DHCP oraz DHCP relay
   2. ***Firewall***
      1. Moduł Firewall musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu
      2. Polityka zabezpieczeń modułu firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzania pasmem.
      3. Moduł firewall musi posiadać możliwość zaraportowania ilości „trafień” wybranej reguły polityki bezpieczeństwa do serwera zarządzania.
      4. Moduł firewall musi pozwalać na konfiguracje reguł polityki bezpieczeństwa z uwzględnieniem okresu czasu w jakim dana reguła będzie aktywna (egzekwowana). Definicja okresu czasu, w ramach którego dana reguła jest aktywna powinna uwzględniać następujące parametry: data i/lub godzina startu, data i/lub godziny zakończenia oraz rekurencyjność.
      5. Moduł firewall musi mieć możliwość automatycznego pobierania, z zewnętrznych serwerów, list z adresami IP i/lub Domenami. Pobranie powinno następować automatycznie i tylko wtedy, gdy treść zewnętrznej listy zostanie zaktualizowana. Funkcjonalność ta musi mieć również możliwość uwierzytelnienia połączenia do zewnętrznego serwera oraz możliwość użycia serwera proxy w celu pobrania listy.
      6. Moduł firewall musi posiadać możliwość konfiguracji reguł polityki bezpieczeństwa w oparciu o tożsamość użytkownika (identity firewall)
      7. Moduł firewall musi domyślnie działać zgodnie z zasadą blokowania całego ruchu sieciowego, poza tym który jest zdefiniowany w regułach polityk bezpieczeństwa i wskazany jako dozwolony
      8. Rozwiązanie musi pozwalać na kontrolę przynajmniej 150 predefiniowanych usług/protokołów
      9. Moduł firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
   3. *Moduł przeciwdziałania próbom włamań (IPS)*
      1. Moduł IPS musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
      2. Moduł IPS musi posiadać możliwość pracy zarówno w trybie pasywnym (Detect) jak i aktywnym (z możliwością blokowania ruchu)
      3. Moduł IPS musi dokonywać inspekcji całych sesji/połączeń. Nie dopuszcza się rozwiązań określających bezpieczeństwo sesji poprzez szczątkową analizę ruchu podczas ustanawiania sesji.
      4. Moduł IPS musi zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:

* sygnatury ataków opartych na exploitach
* reguły oparte na zagrożeniach
* mechanizm wykrywania anomalii w protokołach
  + 1. Moduł IPS musi mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
    2. Moduł IPS musi posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia oraz mieć możliwość zapisywania pakietów generujących zagrożenie
    3. Moduł IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera aktualizacji w sposób uniemożliwiający ich modyfikację podczas przesyłania pomiędzy serwerem aktualizacji oraz serwerem zarządzania/zaporą sieciową.
    4. Moduł IPS musi zapewniać mechanizm zarządzania wersjami bazy sygnatur oraz umożliwiać powrót do wybranej wersji.
    5. Moduł IPS musi posiadać mechanizm automatycznej aktywacji sygnatur minimum w oparciu o następujący zestaw parametrów: poziom zagrożenia, wpływ na wydajność urządzenia, dokładność identyfikacji zagrożenia
    6. Moduł IPS musi zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, IP przeznaczenia lub obu jednoczenie.
    7. Moduł IPS musi zapewniać możliwość obsługi reguł Snort
    8. Moduł IPS musi zapewniać możliwość detekcji i blokowania ataków i zagrożeń opartych na protokole IPv6
    9. Moduł IPS musi pozwalać na objęcie ochroną protokołów SCADA bez potrzeby zakupu dodatkowych licencji
    10. Moduł IPS musi posiadać możliwość aktywowania ochrony dla wybranych zasobów definiowanych minimum w postaci adresów hostów, adresów sieci oraz zakresów adresów IP i przypisywanie do tych zasobów dedykowanych zestawów sygnatur.
    11. Moduł IPS musi posiadać programowy mechanizm pozwalający na wyłączenie ochrony IPS w przypadku wysokiego obciążenia procesora lub pamięci operacyjnej zapory sieciowej. Wartości aktywujące mechanizm muszą być konfigurowalne przez administratora systemu.
    12. Moduł IPS musi posiadać mechanizmy wykrywania i blokowania operacji tunelowania ruchu w wewnątrz innych protokołów, np. DNS tunneling
  1. Moduł kontroli aplikacji
     1. Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 5000 pozycji. Baza modułu powinna być dostępna do weryfikacji online.
     2. Moduł kontroli aplikacji musi posiadać mechanizm ograniczenia użycia pasma dla poszczególnych aplikacji niezależnie dla każdego kierunku przepływu danych (download oraz upload)
     3. Urządzenia Firewall TYP 1 w ramach modułu kontroli aplikacji muszą posiadać możliwość współpracy z modułem analizy treści w zakresie wykrywania i blokowania przesyłania określonych typów danych (np.nr kart kredytowych) oraz określonych typów plików (np. csv, pdf i inne) w ramach zidentyfikowanej aplikacji. W przypadku, kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa.
     4. Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej aplikacji.
     5. Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowanie użytkowników do stron umieszczonych na zewnętrznych serwerach.
     6. System musi umożliwiać administratorom rozszerzenie wbudowanej bazy aplikacji poprzez samodzielne tworzenie nowych sygnatur aplikacji. Jeżeli funkcjonalność ta wymaga dodatkowej licencji to stosowna licencja powinna być dostarczone razem z systemem.
     7. Moduł kontroli aplikacji musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.

* 1. *Moduł identyfikacji użytkowników*
     1. Moduł identyfikacji użytkowników musi umożliwiać uzyskiwanie informacji o tożsamości użytkowników z następujących źródeł:
* integracja z usługą katalogową Microsoft Active Directory
* integracja z usługą Cisco ISE
* identyfikacja w portalu www (captive portal)
* identyfikacja z wykorzystaniem dedykowanego agenta instalowanego na stacji użytkownika
* integracja z serwerem RADIUS
* integracja z serwerem syslog
* połączenia remote access VPN
* integracja z zewnętrznymi systemami IDP z uwzględnieniem protokołu SAML
  + 1. Moduł identyfikacji użytkowników we współpracy z usługą Microsoft Active Directory musi umożliwiać pozyskiwanie informacji o grupach, do których należy zidentyfikowany użytkownik.
    2. Moduł identyfikacji użytkowników musi umożliwiać skuteczną identyfikację użytkowników pracujących z wykorzystaniem serwerów teminali współdzielących pojedynczy adres IP
    3. Moduł identyfikacji użytkowników musi umożliwiać identyfikację użytkowników znajdujących się za urządzeniem typu http proxy poprzez wykorzystanie informacji zawartej w nagłówku X-Forwarded-For. Moduł po pozyskaniu informacji z nagłówka XFF musi go usunąć przed przekazaniem komunikacji do serwera docelowego.
    4. Moduł identyfikacji użytkowników przy współpracy z usługą katalogową Microsoft Active Directory powinien wykorzystywać minimalne wymagane uprawnienia po stronie usługi Active Directory. Niedopuszczalna jest integracja z domeną MS Active Directory w ramach której wymagane jest zastosowanie uprawnień administratora domeny.
    5. Moduł identyfikacji użytkowników musi posiadać możliwość współdzielenia informacji o zidentyfikowanych użytkownikach pomiędzy urządzeniami UTM pochodzącymi od tego samego producenta i zarządzanymi z tego samego lub odrębnego serwera zarządzania
    6. System bezpieczeństwa musi umożliwiać wykorzystanie informacji uzyskanych przez moduł identyfikacji użytkowników w ramach definicji reguł polityki bezpieczeństwa w celu zapewniania użytkownikom lub grupom użytkowników spójnych reguł dostępu do zasobów niezależnie od ich lokalizacji.
  1. *Inspekcja ruchu szyfrowanego (HTTPS, SSH)*
     1. System bezpieczeństwa musi zapewniać mechanizmy inspekcji komunikacji szyfrowanej HTTPS oraz inspekcji komunikacji realizowanej w oparciu o protokół SSH.
     2. System bezpieczeństwa musi pozwalać na inspekcję ruchu HTTPS zarówno dla ruchu wychodzącego z sieci organizacji (np. komunikacja użytkowników z usługami w sieci Internet) jaki i ruchu przychodzącego kierowanego do usług udostępnianych przez organizację. Inspekcja powinna obejmować analizę ruchu pod kątem zgodności z regułami polityki dostępowej (np. kontrola aplikacji oraz kategorii URL) oraz weryfikować ruch pod kątem ewentualnych zagrożeń (np. moduł IPS, moduł antywirusowy).
     3. System musi umożliwiać administratorom zdefiniowanie reguł określających jaka część ruchu HTTPS ma zostać poddana inspekcji, a jaka ma zostać z niej wykluczona. W ramach definiowania reguł administrator musi posiadać możliwość określenia jakie mechanizmy inspekcyjne (moduły) mają zostać wykorzystane podczas analizy ruchu (np. ochrona antywirusowa).
     4. System musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa.
     5. W ramach mechanizmu inspekcji wychodzącego ruchu HTTPS system musi umożliwiać weryfikację stanu certyfikatu cyfrowego serwera docelowego. System musi umożliwiać blokowanie ruchu do określonego serwera docelowego w przypadku kiedy jego certyfikat został unieważniony, wygasł lub nie został podpisany przez zaufany urząd certyfikacji.
     6. System bezpieczeństwa musi umożliwiać tworzenie listy niezaufanych certyfikatów cyfrowych i w efekcie pozwalać na blokowanie ruchu kierowanego do serwerów, które takie certyfikaty wykorzystują.
     7. System bezpieczeństwa musi zapewniać mechanizmy pozwalające na inspekcję szyfrowanej komunikacji SSH. Niedopuszczalne jest aby system do deszyfracji SSH używał jednego globalnego klucza deszyfrującego
  2. *Moduł do realizacji bezpiecznych połączeń zdalnych* 
     1. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w trybie punkt-punkt (site-to-site) oraz zapewniać możliwość dostępu do zasobów dla użytkowników zdalnych (remote access)
     2. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w oparciu o protokół IKEv1 oraz IKEv2
     3. Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w następujących topologiach: full mesh, star, hub-and-spoke
     4. Moduł IPSec VPN musi umożliwiać kreowanie tuneli w oparciu o klucz współdzielony (preshared key) oraz certyfikaty cyfrowe. W przypadku certyfikatów cyfrowych musi istnieć możliwość wykorzystania certyfikatów wystawianych przez wewnętrzny urząd certyfikacji wbudowany w produkt lub przez zewnętrzne urzędy certyfikacji
     5. Moduł IPSec VPN musi umożliwiać uruchomienie mechanizmu split-tunneling dla połączeń od użytkowników zdalnych.
     6. Niedopuszczalne jest aby moduł IPSec VPN ograniczał licencyjnie liczbę tuneli punkt-punkt jakie mogą zostać nawiązane z poziomu zapory sieciowej.
  3. *Moduł filtrowania kategorii URL*
     1. Moduł filtrowania kategorii URL musi posiadać możliwość tworzenia reguł polityki zawierających jednocześnie wiele kategorii URL.
     2. Moduł filtrowania kategorii URL musi dostarczać wbudowane kategorie URL opisujące niebezpieczne witryny kategoryzowane w oparciu o poziom zagrożenia (np. CriticalRisk lub High Risk), a także w oparciu o rodzaj zagrożenia (np. witryny wyłudzające dane lub witryny będące centrami C&C)
     3. Moduł filtrowania kategorii URL musi umożliwiać tworzenie własnych obiektów opisujących witryny URL oraz ich kategoryzowanie.
     4. Moduł filtrowania kategorii URL musi umożliwiać tworzenie obiektów należących do więcej niż jednej kategorii URL.
     5. Moduł filtrowania kategorii URL musi umożliwiać lokalne nadpisywanie domyślnej kategorii URL dla wybranych witryn.
     6. Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej witryny.
     7. Moduł filtrowania kategorii URL musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowania użytkowników do stron umieszczonych na zewnętrznych serwerach.
  4. *Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet*
     1. System zapobiegania komunikacji z sieciami botnet musi umożliwiać wykrycie oraz zablokowanie podejrzanego zachowania w chronionych segmentach sieci
     2. System zapobiegania komunikacji z sieciami botnet w celu identyfikacji podejrzanych zachowań musi wykorzystywać mechanizmy zabezpieczeń oparte o reputację adresów IP, URL oraz DNS w połączeniu z wykrywaniem wzorców ruchu specyficznych dla połączeń kierowanych do serwerów C&C.
     3. System zapobiegania komunikacji z sieciami botnet musi posiadać możliwość identyfikacji urządzeń wewnętrznych będących źródłem podejrzanych zapytań DNS w przypadku kiedy wykorzystują one wewnętrzny serwer DNS pośredniczący w generowaniu zapytań. Mechanizm musi umożliwiać modyfikację/fałszowanie odpowiedzi DNS i przekierowywanie urządzeń do wcześniej ustalonego adresu IP (tzw. DNS malware trap lub DNS Sinkhole).
     4. Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, FTP, SMB/CIFS, SFTP/SCP
     5. Moduł ochrony antywirusowej musi umożliwiać skanowanie adresów URL oraz załączników znajdujących się w wiadomościach poczty elektronicznej.
     6. Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych (wymagane dla Firewall TYP 1). Administrator musi mieć możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji (przekaż lub zablokuj) która zostanie podjęta w momencie przekroczenia zdefiniowanego limitu.
     7. Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji.
     8. Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet muszą posiadać możliwość interakcji z użytkownikami w zakresie informowania o zablokowaniu dostępu do niebezpiecznych zasobów.
     9. System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) w formacie pliku CSV lub STIX XML (STIX 1.0).
  5. *Moduł ochrony przed atakami 0-day*
     1. Moduł musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, IMAP, FTP, CIFS, SMB
     2. Moduł musi zapewniać możliwość analizowania następujących typów plików:

* + - .7z - 7z Archive
    - .bz2 - bzip2 compressed archive
    - .CAB - Compressed archive
    - .csv - Comma-separated values file
    - .doc Microsoft Word 97-2003 Document
    - .docx Microsoft Word Document
    - .gz - Gz Archive
    - .iso -
    - .jar - Java Browser Applet
    - .pdf - Adobe Acrobat document
    - .ppt - Microsoft PowerPoint 97-2003 Presentation
    - .pptx - Microsoft PowerPoint Presentation
    - .rar - Rar Archive
    - .rtf - Rich Text Format file
    - .swf - Flash
    - .tar - Tar Archive
    - .tgz - Tgz Archive
    - .xls - Microsoft Excel 97-2003 Worksheet
    - .xlsx - Microsoft Excel Worksheet
    - .zip - Zip Archive"
    1. Moduł musi umożliwiać otwarcie dostarczonego za pośrednictwem wspieranych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w tym systemie a następnie podjęcie akcji (zablokuj/przekaż do odbiorcy) w zależności od uzyskanych wyników analizy. Szczegółowy wynik analizy powinien zostać udokumentowany w formie raportu i przesłany na wskazany serwer logów.
    2. Niedopuszczalne jest przekazanie pliku do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym potwierdzającego że analizowany plik jest bezpieczny. Wyjątkiem jest dostarczenie do użytkownika bezpiecznej wersji pliku, tzn. wersji pozbawionej całej treści aktywnej. Jako treść aktywna rozumiane są między innymi makra pakietu MS Office, odnośniki do zewnętrznych zasobów, obrazy, kwerendy do baz danych, skrypty JavaScript, filmy i inne.
    3. Moduł musi umożliwiać wykonywanie analizy zachowania plików w środowiskach wirtualnych opartych o różne wersje systemu operacyjnego Microsoft Windows oraz różne pakiety oprogramowania Microsoft Office. Licencja dostarczona wraz z modułem musi zawierać prawa do użytkowania zewnętrznego oprogramowania zawartego w obrazach systemów do celów analizy plików w środowiskach wirtualnych.
    4. Moduł w ramach analizy plików w środowiskach wirtualnych powinien monitorować minimum następujące aktywności:
* zapytania API
* zmiany w systemie plików (np. tworzenie i usuwanie plików, modyfikowanie uprawnień do plików)
* zmiany w rejestrze systemowym
* próby nawiązania połączeń sieciowych
* próby eskalacji uprawnień
* próby ominięcia systemu UAC
  + 1. Moduł musi umożliwiać wykrywanie zagrożeń na etapie przełamywania zabezpieczeń systemu (exploit).
    2. Moduł musi umożliwiać analizowanie plików wskazywanych poprzez odnośniki znajdujące się w analizowanych wiadomościach pocztowych.
    3. Moduł musi posiadać mechanizm pozwalający na przekazywanie informacji o wykryciu niebezpiecznego pliku do chmury producenta w celu wygenerowania sygnatury.
    4. Moduł musi umożliwiać wykonywanie analizy plików w środowiskach wirtualnych uruchamianych w chmurze producenta lub na lokalnym, dedykowanym urządzeniu dostarczonym przez producenta. W przypadku analizy plików w środowisku chmurowym musi istnieć możliwość określenia obszaru geograficznego w jakim zlokalizowane są centra danych producenta do ktorych przesyłane będą pliki. Minimum wymagana jest możliwość ograniczenia obszaru geograficznego do terenu Unii Europejskiej (GDPR).
    5. Zamawiający nie wymaga dostarczenia dedykowanego urządzenia do wykonywania analizy plików lokalnie.
    6. Moduł musi posiadać mechanizmy pozwalające na dynamiczną analizę aplikacji www w celu ciągłej weryfikacji ataków typu web phishing. Analiza powinna być wykonywana w sposób ciągły w momencie próby dostępu do aplikacji www przez użytkownika (wymagane dla Firewall Typ 1)
    7. Moduł musi posiadać mechanizmy chroniące przed atakami typu DNS Data Exfiltration:
* Domain Generation Algorithm
* Domain Name System Tunneling
  + 1. Moduł musi umożliwiać analizę stron www w celu wykrycia ataków 0-day phishing. Niedopuszczalne jest, aby rozwiązanie korzystało tylko z czarnych/białych list lub kategorii URL w celu wykrywania stron phishingowych, Producent musi udostępniać informacje o stronach 0-day phishing wykrytych przez oferowane rozwiązanie producenta.
  1. ***Firewall TYP 1 - wymagania sprzętowe*** 
     1. Urządzenia pełniące rolę zapory sieciowej muszą być przystosowane do zamontowania w szafie RACK 19” lub posiadać dostarczaną przez producenta półkę umożliwiająca taki montaż. Dodatkowo muszą zostać dostarczone wraz z niezbędnym do montażu sprzętem i okablowaniem oraz licencją na zewnętrzny centralny system zarządzania.
     2. Wysokość obudowy urządzenia nie może być większa niż 1U.
     3. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w pamięć DRAM nie mniejszą niż 32GB.
     4. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w dysk SSD o pojemności nie mniejszej niż 480GB.
     5. Urządzenie pełniące rolę zapory sieciowej musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 4,8 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day) i obsługiwać nie mniej niż 7 000 000 jednoczesnych połączeń z możliwością obsługi przyrostu 190 000 połączeń na sekundę.
     6. Podane w punkcie 2.11.5 parametry przepływności dotyczą wydajności zapory sieciowej w warunkach typu Enterprise. Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab” „ideal” itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne.
     7. Każde urządzenie musi być wyposażone w co najmniej:
     + 8 portów 1Gbps RJ45, przeznaczone do ruchu produkcyjnego.
     + 8 portów 1/10Gbps SFP+ obsadzonych wkładkami 10G SR, przeznaczone do ruchu produkcyjnego
     1. Każde z urządzeń pełniących rolę zapory sieciowej musi być wyposażone w redundantne zasilacze zasilanie prądem przemiennym 230V (niedopuszczalne są rozwiązania zewnętrzne).
     2. Każde urządzenie musi być wyposażone w moduł do zarządzania out-of-band (tzw. LOM), który pozwala na obsługę zdalną urządzenia co najmniej w poniższy sposób:
     + Instalacja systemu,
     + Restart urządzenia,
     + Wyłączenie urządzenia,
     + Włączenie urządzenia,
     + Dostęp do portu konsoli urządzenia.
     1. Oferent zobowiązany jest do dostarczenia dwóch urządzeń spełniających wymagania opisane w punktach 2.11.1 – 2.11.9
  2. ***Firewall TYP 2 - wymagania sprzętowe*** 
     1. Urządzenia pełniące rolę zapory sieciowej muszą być przystosowane do zamontowania w szafie RACK 19” lub posiadać dostarczaną przez producenta półkę umożliwiająca taki montaż. Dodatkowo muszą zostać dostarczone wraz z niezbędnym do montażu sprzętem i okablowaniem oraz licencją na zewnętrzny centralny system zarządzania.
     2. Wysokość obudowy urządzenia nie może być większa niż 1U.
     3. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w pamięć DRAM nie mniejszą niż 16GB.
     4. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w dysk SSD o pojemności nie mniejszej niż 480GB.
     5. Urządzenie pełniące rolę zapory sieciowej musi posiadać przepływność w ruchu full-duplex nie mniej niż 8 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 4 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń z możliwością obsługi przyrostu 89 000 połączeń na sekundę.
     6. Podane w punkcie 2.12.4 parametry przepływności dotyczą wydajności zapory sieciowej w warunkach typu Enterprise. Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab” „ideal” itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne.
     7. Każde urządzenie musi być wyposażone w co najmniej:
        + 16 portów 1Gbps RJ45, przeznaczonych do ruchu produkcyjnego.
        + 4 porty 10Gbps SFP+ obsadzone wkładkami 10G SR, przeznaczone do ruchu produkcyjnego.
     8. Każde z urządzeń pełniących rolę zapory sieciowej musi być wyposażone w redundantne zasilacze zasilanie prądem przemiennym 230V (niedopuszczalne są rozwiązania zewnętrzne).
     9. Oferent zobowiązany jest do dostarczenia dwóch urządzeń spełniających wymagania opisane w punktach 2.12.1 – 2.12.8

1. ***Moduł zarządzania (specyfikacja)***
   1. *Wymagania funkcjonalne*
      1. Moduł zarządzania musi mieć możliwość zarządzania minimum dziesięcioma punktami wymuszania polityki bezpieczeństwa (urządzeniami UTM)
      2. Moduł zarządzania musi umożliwiać jednoczesną pracę wielu administratorów - w tym także jednoczesną pracę w ramach pojedynczej polityki bezpieczeństwa.
      3. Moduł zarządzania musi zapewniać możliwość tworzenia wielu różnych polityk bezpieczeństwa oraz umożliwiać ich przypisanie do poszczególnych urządzeń UTM zarządzanych z poziomu serwera.
      4. Moduł zarządzania musi umożliwiać tworzenie modułowej polityki bezpieczeństwa. System musi umożliwiać współdzielenie modułów (zestawów reguł polityki bezpieczeństwa) pomiędzy różnymi politykami bezpieczeństwa.
      5. Moduł zarządzania musi posiadać mechanizmy automatycznej weryfikacji spójności i niesprzeczności implementowanej polityki bezpieczeństwa przed zainstalowaniem jej na urządzeniach UTM.
      6. Moduł zarządzania musi posiadać mechanizmy pozwalające na weryfikację poprawności działania nowej wersji polityki bezpieczeństwa po jej uruchomieniu na urządzeniu UTM oraz możliwość automatycznego powrotu do poprzedniej wersji w przypadku stwierdzenia nieprawidłowości na bazie zestawu testów utworzonych przez administratora- np. brak dostępu do wybranych usług powstały w wyniku błędu administratora
      7. Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa, możliwość porównywania różnych wersji polityki pod kątem różnic między nimi, a także opcję cofnięcia konfiguracji do wybranej wersji.
      8. Moduł zarządzania musi zapewniać możliwość uwierzytelnianie administratorów za pomocą haseł statycznych, haseł dynamicznych, certyfikatów cyfrowych oraz protokołu SAML.
      9. Moduł zarządzania musi zapewniać możliwość definiowania szczegółowych zestawów uprawnień dla poszczególnych administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
      10. Moduł zarządzania musi posiadać mechanizmy zapewniające rozliczalność zmian konfiguracyjnych wykonanych przez poszczególnych administratorów w formie generowania i przechowywania logów audytowych. Logi muszą zawierając minimum informacje o tożsamości administratora oraz czasie i zakresie wykonywanych zmian.
      11. Moduł zarządzania musi posiadać mechanizm sprawdzania i zatwierdzania zmian dokonanych przez administratora (umownie administratora poziomu 1) przez innego administratora (umownie administratora poziomu 2) przed instalacja polityki. Mechanizm ten powinien mieć możliwość notyfikacji administratora poziomu 2, że zmiany w polityce/konfiguracji czekają na zatwierdzenie. Funkcjonalność ta powinna być dostępna z systemu zarządzania bez dodatkowej licencji.
      12. Moduł zarządzania musi posiadać mechanizmy centralnego zarządzania licencjami dla wszystkich komponentów wchodzących w skład systemu bezpieczeństwa (serwery logów, serwery korelacji zdarzeń i raportowania, zapory sieciowe)
      13. Moduł zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych urządzeń UTM takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa
      14. Moduł zarządzania musi posiadać dedykowane API umożliwiające automatyzację czynności administracyjnych. Mechanizm API powinien umożliwiać minimum wykonanie następujących czynności:

* tworzenie, edycja oraz usuwanie obiektów sieciowych i usług
* tworzenie, modyfikowanie oraz usuwanie reguł polityki bezpieczeństwa oraz reguł NAT
* instalacja polityki bezpieczeństwa
* zarządzania kontami administratorów systemu
  + 1. Moduł zarządzania musi realizować funkcję serwera logów w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych urządzeń UTM. W ramach funkcji serwera logów muszą istnieć wbudowane mechanizmy ochrony przestrzeni dyskowej przed przepełnieniem Mechanizm powinien umożliwiać wykonywanie różnych akcji systemu w zależności od poziomu zajętości dysku. Możliwe akcje to minimum wysyłanie alertów do administratorów oraz automatyczne usuwanie najstarszych plików logów
    2. Moduł zarządzania musi posiadać mechanizmy pozwalające na implementację rozwiązania wysokiej dostępności, w ramach której możliwe jest dodanie zapasowego serwera zarządzania oraz uruchomienie automatycznej synchronizacji konfiguracji polityk bezpieczeństwa. Dostarczenie zapasowego serwera zarządzania nie jest wymagane w ramach postępowania.
    3. Moduł zarządzania musi mieć możliwość wykrywania incydentów bezpieczeństwa na bazie logów pochodzących z dziesięciu zarządzanych urządzeń UTM.
    4. Moduł zarządzania musi pozwalać na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych bez konieczności definiowania wartości dla poszczególnych atrybutów (tzw.freetext search).
    5. Moduł zarządzania musi pozwalać na grupowanie wyników wyszukiwania logów/incydentów bezpieczeństwa według określonych atrybutów (minimum typ incydentu, zasoby, nazwa użytkownika).
    6. Moduł zarządzania musi umożliwiać wykonywanie analizy incydentów bezpieczeństwa od poziomu ogólnego do szczegółowych logów odpowiedzialnych za wygenerowanie zdarzenia (tzw. drill-down).
    7. Moduł zarządzania musi umożliwiać administratorom tworzenie własnych raportów oraz ekranów (formatka prezentująca określony podzbiór danych w formie zdefiniowanej przez administratora), a także modyfikowanie raportów i widoków dostarczonych razem z systemem.
    8. Moduł zarządzania musi umożliwiać graficzną prezentację danych w zakresie logów oraz zidentyfikowanych incydentów bezpieczeństwa.
    9. Moduł logów zarządzania musi umożliwiać filtrowanie /incydentów bazując na parametrach takich jak: aplikacja, źródłowy i docelowy IP, usługa, typ zdarzenia, istotność ataku, kraj pochodzenia itd.
    10. Moduł zarządzania musi posiadać możliwość budowania własnych raportów przez administratorów w trybie na żądanie oraz zgodnie z zadanym harmonogramem.
    11. Moduł zarządzania musi umożliwiać współdzielenie własnych/customowych raportów pomiędzy administratorami.
    12. Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF oraz CSV. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców.
    13. Moduł zarządzania musi posiadać możliwość tworzenia niestandardowych reguł korelacji zdarzeń bezpieczeństwa.
    14. Moduł zarządzania musi posiadać możliwość konfigurowania automatycznych reakcji na wykryte incydenty bezpieczeństwa - minimum w postaci wysłania wiadomość e-mail, wygenerowanie SNMP trap lub uruchomienie skryptu
    15. Zamawiający dopuszcza realizację funkcjonalności modułu zarządzania opisanych w punktach 3.1.15.-3.1.28 przez więcej niż jedną maszynę wirtualną lub fizyczną, jeżeli taka potrzeba wynika z architektury oferowanego rozwiązania.
    16. Zamawiający dopuszcza realizację funkcjonalności modułu zarządzania opisanych w punktach 3.1.1.-3.1.28 przy zastosowaniu platformy sprzętowej lub wirtualnej. Każda platforma, niezależnie od typu, powinna zapewniać minimalnie 2TB powierzchni dyskowej oraz umożliwiać zapis minimum 10GB logów.

Jeśli w opisie przedmiotu zamówienia występują: nazwy konkretnego producenta, nazwy konkretnego produktu, normy jakościowe, patenty, znaki towarowe, typy, standardy należy to traktować jedynie jako pomoc w opisie przedmiotu zamówienia. W każdym przypadku dopuszczalne są produkty równoważne pod względem konstrukcji, materiałów, funkcjonalności, jakości. Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent czy pochodzenie, to należy przyjąć, że wskazane patenty, znaki towarowe, pochodzenie określają parametry techniczne, eksploatacyjne, użytkowe, co oznacza, że Zamawiający dopuszcza złożenie ofert w tej części przedmiotu zamówienia o równoważnych parametrach technicznych, eksploatacyjnych i użytkowych. Obowiązek wykazania równoważności spoczywa na Wykonawcy, który w przypadku oferowania rozwiązań równoważnych powinien dołączyć do oferty specyfikacje techniczne, karty katalogowe, instrukcje lub inne dokumenty zawierające dane techniczne elementów równoważnych. W razie wątpliwości co do równoważności poszczególnych elementów, Zamawiający wezwie Wykonawcę do złożenia dodatkowych wyjaśnień lub dokumentów

W ramach usług należy wykonać :

1. Montaż i uruchomienie sprzętu oraz licencji.
2. Uruchomienie polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
3. Dokumentację powdrożeniową.

Całość musi zostać objęta 36 miesięcznym serwisem i wsparciem producenta

1. Warunki udziału w postępowaniu.
   1. Wiedza i doświadczenie :

Oferent posiada wiedzę i doświadczenie niezbędne do realizacji przedmiotu zamówienia tj.:

* zrealizował co najmniej 2 inwestycje polegające na zabezpieczeniu sieci komputerowych LAN z użyciem firewalli w technologii clustra niezawodnościowego o wartości każdej z nich na minimum 300 000,00 zł,
  1. Uprawnienia do wykonywania określonej działalności lub czynności.
  2. Potencjał techniczny.

Oferent dysponuje odpowiednim potencjałem technicznym niezbędnym do realizacji

przedmiotu zamówienia.

* 1. Osoby zdolne do wykonania zamówienia.
* Oferent dysponuje osobami zdolnymi do wykonania przedmiotu zamówienia co najmniej 2 inżynierów certyfikowanych w oferowanej technologii.

1. Sytuacja ekonomiczna i finansowa

3.1. Oferent pozostaje w sytuacji ekonomicznej i finansowej pozwalającej na realizację pełnego zakresu przedmiotu zamówienia tj.:

* powinien dostarczyć zaświadczenia z ZUS i US o niezaleganiu z należnościami wobec Skarbu Państwa,
* powinien dostarczyć kopię ubezpieczenia OC działalności na sumę co najmniej o wartości zaoferowanej ceny przedmiotu zamówienia,
* powinien dostarczyć gwarancję bankową na zabezpieczenie należytego wykonania przedmiotu umowy w wysokości 10 % wartości kontraktu,

1. Kryteria oceny oferty:

* Cena netto bez usług, wykazana w ofercie za realizację pełnego przedmiotu zamówienia (sprzęt + licencje)
* Osobno cena usług.
* Obecność producenta sprzętu i oprogramowania wśród liderów w branży bezpieczeństwa IT.
* Warunki serwisu.
* Zagwarantowanie kompletności zrealizowania wszystkich wymagań funkcjonalnych zawartych w punktach 1,2,3.

1. Informacja o wagach punktowych lub procentowych przypisanych do poszczególnych kryteriów oceny oferty

* Cena netto wykazana w ofercie za realizację pełnego przedmiotu zamówienia 30%
* Cena usług 20%
* Obecność producenta sprzętu i oprogramowania wśród liderów w branży bezpieczeństwa IT 20%
* Warunki serwisu 10%
* Zagwarantowanie kompletności zrealizowania wszystkich wymagań funkcjonalnych 20% (Punkty 1,2,3 specyfikacji)

1. Opis sposobu przyznawania punktacji za spełnienie danego kryterium oceny oferty
2. Kryterium „Cena netto” (Kc) będzie obliczane na podstawie wzoru: Kc = Cn/Co x 30% x 100 punktów, gdzie:

Cn – najniższa zaproponowana cena netto

Co – cena netto zaproponowana w badanej ofercie

Kc – liczba punktów

1. Kryterium „Cena usług” (Kc) będzie obliczane na podstawie wzoru: Kc = Cn/Co x 20% x 100 punktów, gdzie:

Cn – najniższa zaproponowana cena netto

Co – cena netto zaproponowana w badanej ofercie

Kc – liczba punktów

1. Obecność producenta rozwiązania wśród liderów Kwadratu Gartnera lub innego uznanego międzynarodowego rankingu bezpieczeństwa IT: (1 za TAK lub 0 za NIE) x 10% x 100 punktów
2. Warunki serwisu: (1-2 za TAK lub 0 za NIE) x 10% x 100 punktów

Gwarancja minimum 2 lata – 2%

Serwis 6-22 dostępność – 2%

Komunikacja w języku polskim – 2%

Czas przyjęcia zgłoszenia i reakcji (tj. zalogowani się do systemu i diagnozy) 4h – 2%

Czas przywrócenia systemu do poprawnego działania (max 2%):

- w ciągu 24h – 2%,

- w ciągu 48h – 1%,

1. kompletności zrealizowania wszystkich wymagań funkcjonalnych

gwarancja realizacji powyżej 95% wszystkich kryteriów – 20 punktów

gwarancja realizacji pomiędzy 80-95 % kryteriów – 5 punktów

gwarancja realizacji poniżej 80% kryteriów – 0 punktów

1. Termin składania ofert: 31 dni tj. do dnia 20.01.2025 r.

Bieg terminu rozpoczyna się w dniu następującym po dniu upublicznienia zapytania ofertowego, a kończy się z upływem ostatniego dnia. Jeżeli koniec terminu przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następującego po dniu lub dniach wolnych od pracy

1. Zamawiający nie przewiduje możliwości składania ofert częściowych.
2. Zamawiający przewiduje możliwość dokonywania zamówień uzupełniających
3. Termin realizacji umowy: 4 miesiące od daty zawarcia umowy.
4. Zamawiający przewiduje możliwość zmiany zapisów umowy po wyrażeniu zgody przez

Zamawiającego i podpisaniu aneksu do umowy.

Zmiany zapisów umowy będą mogły być wprowadzane z powodu:

- jeśli okaże się to konieczne ze względu na zmianę przepisów powszechnie obowiązującego prawa po zawarciu umowy w zakresie niezbędnym do dostosowania Umowy do zmienionych przepisów;

- zmiany umownego terminu wykonania umowy lub sposobu wykonania przedmiotu zamówienia, gdy zaistnieje niemożliwa do przewidzenia w momencie zawarcia umowy okoliczność prawna, ekonomiczna lub wystąpi siła wyższa, za którą żadna ze stron nie ponosi odpowiedzialności, skutkująca brakiem możliwości należytego wykonania zawartej umowy   
w umownym terminie oraz na skutek zmiany zasad finansowania projektu wynikającego   
z podpisanych przez Zamawiającego umów z Instytucjami.

1. Warunki ewentualnego odstąpienia od zawarcia umowy

Zamawiający zastrzega sobie prawo odstąpienia od zawarcia umowy z wybranym wykonawcą w sytuacji wycofania się z realizacji projektu, a także w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu sporządzania niniejszego zapytania Ofertowego.

INFORMACJA DODATKOWE:

1. Postępowanie na wybór wykonawcy zamówienia w projekcie jest prowadzenie zgodnie   
   z Regulaminem wyboru przedsięwzięć do objęcia wsparciem z planu rozwojowego w trybie konkursowym Załącznik nr 6: Zasada konkurencyjności w ramach inwestycji A 2.1.1, w tym   
   z zachowaniem zasad uczciwej konkurencji oraz równego traktowania wykonawców.
2. Zamawiający zastrzega sobie prawo unieważnienia zapytania ofertowego bez podania przyczyny.
3. Zamawiający może zmienić Zapytanie ofertowe, przed upływem terminu składania ofert,   
   a o zakresie zmian poinformuje w Zapytaniu ofertowym. Zamawiający może przedłużyć termin składania ofert o czas niezbędny do wprowadzenia zmian w ofertach, jeżeli jest to konieczne   
   z uwagi na zakres wprowadzonych zmian.
4. Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
5. Z zawartością ofert nie można zapoznać się przed upływem terminu otwarcia ofert.
6. Zamawiający poinformuje o wynikach postępowania za pośrednictwem swojej strony internetowej.
7. Po dokonaniu wyboru oferty Zamawiający poinformuje Oferenta, którego ofertę wybrano   
   o terminie podpisania umowy.
8. Przedmiotowa oferta musi spełniać wszystkie wymienione wymagania i warunki postawione   
   w Zapytaniu ofertowym i przedmiocie zamówienia.
9. Zamawiający może w toku badania i oceny ofert zażądać od Oferentów dodatkowych wyjaśnień dotyczących treści złożonych ofert, w tym dokumentów potwierdzających podane w ofercie informacje.
10. Zamawiający dopuszcza możliwość prowadzenia negocjacji z Oferentami.
11. Terminy płatności: 30 dni od daty wpływu faktury do siedziby Zamawiającego. Ilość faktur: 2 w trakcie realizacji zamówienia.
12. LISTA WYMAGANYCH DOKUMENTÓW/OŚWIADCZEŃ:
13. Oferta powinna zawierać:

- wypełniony i podpisany Formularz ofertowy stanowiący Załącznik nr 1 do Zapytania ofertowego,

- wypełnione i podpisane Oświadczenie o braku powiązań osobowych i kapitałowych   
z Zamawiającym stanowiące Załącznik nr 2 do Zapytania ofertowego,

- informację na temat oferowanego przedmiotu zamówienia,

- dokumentację potwierdzającą posiadanie Certyfikatów dot. warunku udziału Uprawnienia do wykonywania określonej działalności lub czynności,

- dokumentacja oraz referencje potwierdzające spełnienie warunku udziału Wiedza i doświadczenie,

- dokumentacja potwierdzająca spełnienie warunku udziału Sytuacja ekonomiczna i finansowa,

- inne zgodnie ze sposobem przygotowania oferty.

1. Oferty należy przesłać e-mailem jednocześnie na dwa adresy: [zbigniew.koplin@piatnica.com.pl](mailto:zbigniew.koplin@piatnica.com.pl) i karol.gardocki@piatnica.com.pl