Nazwa	Wymagane parametry techniczne
Opis	System proaktywnej ochrony przed zaawansowanymi zagrożeniami - którego zadaniem będzie wykrywanie i blokowanie ataków w infrastrukturę sieci, a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. System powinien umożliwiać lokalne logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania. Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API (np. icap). Musi istnieć możliwość pełnej integracji z urządzeniami będącymi w posiadaniu przez Zamawiającego **Fortigate 1100E, Fortimail, Fortianalyzer.** Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania. Urządzenie fabrycznie nowe i pochodzące z autoryzowanego kanału producenta.
System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu musi pracować w oparciu o dedykowany, wzmocniony system operacyjny z punktu widzenia bezpieczeństwa.
Parametry fizyczne systemu	System musi zapewniać: – 4 interfejsy Ethernet 10/100/1000, – Powierzchnie dyskową - minimum 1 TB. W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia. Elementy systemu o maksymalnej wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Funkcjonalności podstawowe i uzupełniające	Ochrona przez zaawansowanymi atakami: 1. Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM. 2. Procesowanie plików o rozmiarze co najmniej 8 MB. 3. Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR). 4. Plików multimedialnych: .avi, .mpeg, .mp3, .mp4. 5. Skanowane protokoły sieciowe: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowania ruchu o przepływności 500 Mbps. 6. Skanowanie stron www z linkami URL. 7. Czarne i białe listy dla sum kontrolnych plików. 8. Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, kopii migawkowej (snapshotu) VM. 9. Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap.
Parametry wydajnościowe	Możliwość uruchomienia min. 6 instancji wirtualnych systemów MS Windows zawierających Windows 7, Windows 8 i Windows 10 oraz 1 pakiet biurowy MS Office w celu wykonania analizy Sandbox w wymiarze co najmniej 120 plików na godzinę.
Zarządzanie	1. Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. 2. Dostęp do CLI przez SSH.
Serwisy	1. Gwarancja i serwis producenta na okres 36 miesięcy. 2. Subskrypcja funkcji bezpieczeństwa Antivirus, IPS, Web Filtering na okres: 36 miesięcy.
Usługi wdrożenia	Usługa wdrożenia obejmie poniższe elementy: – inicjalizacja urządzenia, – aktualizacja firmware, – instalacja maszyn wirtualnych, – konfiguracja polityk skanowania, – integracja z NGFW i Email Security Gateway (Fortigate, Fortimail, FortiAnalyzer), – przegląd logów systemowych, wskazanie potencjalnych zagrożeń, – szkolenie z obsługi urządzenia, – przygotowanie dokumentacji powdrożeniowej.