

NZ.231.124.2017.JŚ

Katowice, dnia 16.11.2017r.

## WYJAŚNIENIA I ZMIANA TREŚCI SIWZ

*Dostawa urządzeń klasy UMT/NextGen Firewall, oprogramowania antywirusowego, sprzętu komputerowego oraz materiałów eksploatacyjnych  
(4 części)*

W związku z wpłynięciem wniosku o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia, Zamawiający na podstawie art. 38 ust. 1 i 2 ustawy Prawo zamówień (Dz. U. 2017, poz. 1759 ze zmianami) zamieszcza treść pytań oraz udziela wyjaśnień oraz zmienia treść Specyfikacji Istotnych Warunków Zamówienia.

**Część 1** dostawa urządzenia UMT/NextGen Firewall - dotyczy Załącznika Nr 1.1.A do SIWZ:

**Pytanie 1.** Wnioskujemy o zmianę:

Obsługa trybów pracy: routera (każdy port obsługuje inny adres sieci/podsieci IP), bridge (transparent mode) lub z tym samym adresem IP na wszystkich portach na:  
Obsługa trybów pracy: Router/NAT lub transparent.

**Odp. 1- Zamawiający dokonuje zmiany zapisu na:**

Obsługa trybów pracy: Router/NAT lub transparent.

**Pytanie 2.** Wnioskujemy o zmianę:

Rozpoznawanie oraz uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników w tym transparentne uwierzytelnianie użytkowników przez Active Directory na:

Rozpoznawanie oraz uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius oraz wewnętrznej bazy użytkowników w tym transparentne uwierzytelnianie użytkowników przez Active Directory;

**Odp. 2- Zamawiający dokonuje zmiany zapisu na:**

Rozpoznawanie oraz uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius oraz wewnętrznej bazy użytkowników w tym transparentne uwierzytelnianie użytkowników przez Active Directory;

**Pytanie 3.** Wnioskujemy o zmianę:

Funkcjonalność pracy w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP na:

Funkcjonalność pracy w trybie DHCP Relay.

**Odp. 3- Zamawiający dokonuje zmiany zapisu na:**

Funkcjonalność pracy w trybie DHCP Relay.

**Pytanie 4.** Wnioskujemy o zmianę:

Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów min: IPSec, SSL, L2TP na:  
Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów min: IPSec, SSL.

**Odp. 4- Zamawiajcy dokonuje zmiany zapisu na:**

Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów min: IPSec, SSL;

**Pytanie 5.** Wnioskujemy o zmianę:

Oprogramowanie klienta SSL VPN musi być dostępne dla platform: Windows 7, 8 i 10, MacOS, iOS i Android na:

Oprogramowanie klienta SSL VPN musi być dostępne dla platform: Windows 7, 8 i 10;

**Odp. 5- Zamawiajcy dokonuje zmiany zapisu na:**

Oprogramowanie klienta SSL VPN musi być dostępne dla platform: Windows 7, 8 i 10;

**Pytanie 6.** Wnioskujemy o zmianę:

Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według podziału na kategorie (min 100 kategorii składowanych lokalnie lub z uwzględnieniem filtrów dostępnych w chmurze) na:

Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według podziału na kategorie (min 50 kategorii składowanych lokalnie lub z uwzględnieniem filtrów dostępnych w chmurze);

**Odp. 6- Zamawiajcy dokonuje zmiany zapisu na:**

Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według podziału na kategorie (min 65 kategorii składowanych lokalnie lub z uwzględnieniem filtrów dostępnych w chmurze);

**Pytanie 7.** Wnioskujemy o zmianę:

Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online na:

Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online;

**Odp. 7- Zamawiajcy dokonuje zmiany zapisu na:**

Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, Proxy service, Peer-to-peer, Komunikatory, Portale społecznościowe, Gry online;

**Pytanie 8.** Wnioskujemy o zmianę:

Urządzenie powinno mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV na:

Urządzenie powinno mieć możliwość eksportowania raportów do pliku CSV;

**Odp. 8- Zamawiajcy dokonuje zmiany zapisu na:**

Możliwość generowania raportów w formacie PDF, oraz opcja eksportowania szczegółowych informacji do plików min. CSV z poziomu urządzenia fizycznego lub wirtualnego;

**Pytanie 9.** Czy zamawiający dopuszcza urządzenie które posiada przepustowość VPN na poziomie 1,7 Gbps, oraz IPS na poziomie 4,2 Gbps?

**Odp. 9 - Zamawiajcy dopuszcza obniżenie parametru przepustowości VPN do min. 2,5 Gb/s i dokonuje zmiany zapisu:**

Przepustowość VPN: min. 4 Gb/s;

na:

Przepustowość VPN: min. 2,5 Gb/s;

**Pytanie 10.** Proszę o wyrażenie zgody na dopuszczenie rozwiązania które nie spełnia poniższych zapisów:

Agent instalowany na końcówkach użytkowników:

- agent wykrywający i zbierający informacje o zagrożeniach występujących na końcówkach (komputery, serwery);
- korelacja zdarzeń związanych z bezpieczeństwem sieci z konkretnymi końcówkami generującymi te zdarzenia;
- przysyłanie informacji o zagrożeniach wykrytych na końcówkach do urządzenia lub serwisu zlokalizowanego w chmurze z informacjami odnoszącymi się do plików, procesów, połączeń sieciowych i kluczy rejestru;
- możliwość wykonania instalacji agentów z wykorzystaniem struktury Active Directory;

**Odp. 10** - W/w parametry dotyczą oprogramowania klienta, którego dostawa nie jest wymagana obligatoryjnie, jest wymaganiem opcjonalnym/dodatkowym, punktowanym dodatkowo w ramach dostarczenia aplikacji agenta przeznaczonego do instalowania na stacjach roboczych i współpracującego z urządzeniem. W związku z tym, Wykonawca może dostarczyć urządzenie, bez licencji agenta o którym mowa powyżej.

**Pytanie 11.** - Zarządzanie

- Edytowanie polityk bezpieczeństwa w trybie online oraz edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według harmonogramu;
- Możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty);

**Odp. 11** - Zamawiający wyraża zgodę na dostawę urządzenia nie spełniającego w/w wymagań i w związku z tym dokonuje usunięcia w/w zapisów z zał. 1.1.A.

**Pytanie 12.** - Dzienniki i raporty

Brak ograniczeń co do czasu przechowywania oraz wielkości bazy logów;

**Odp.** - Zamawiający podtrzymuje zapisy specyfikacji

System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.

**Odp.** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

Logi urządzenia muszą być gromadzone nieprzerwanie od momentu wdrożenia urządzenia i dostępne w zadanych okresach czasowych;

**Odp.** - Zamawiający dokonuje zmiany w/w zapisu na:

Możliwość gromadzenia logów urządzenia nieprzerwanie od momentu wdrożenia urządzenia;

W wypadku dostępnej dedykowanej maszyny wirtualnej gromadzącej logi generowane przez urządzenie, pojemność plików logów przechowywanych na tej maszynie ograniczana postanowieniami licencyjnymi narzuconymi przez producenta nie może być mniejsza niż 1TB – cena ewentualnej licencji na użytkowanie tej maszyny (jeśli jest wymagana) musi zostać zawarta w ofercie Dostawcy;

**Odp.** - Zamawiający podtrzymuje zapisy specyfikacji

**Pytanie 13.** Funkcje VPN

Urządzenie ma posiadać certyfikat ICSA IPSec VPN;

**Odp. 13** - Zamawiający dokonuje zmiany w/w zapisu na:

Urządzenie ma posiadać certyfikat ICSA IPSec VPN lub certyfikaty równoważne;

**Pytanie 14.** - Funkcjonalność Firewall

Funkcjonalność pracy w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP;

**Odp. 14** - Zamawiający dokonuje zmiany zapisu na:

Funkcjonalność pracy w trybie DHCP Relay.

**Pytanie 15.** - Jeden z wymogów wskazanych przez Zamawiającego to:

Urządzenie dostarczone z najbogatszym pakietem funkcjonalności (subskrypcji) oferowanym przez producenta w dniu dostawy, obowiązującym w okresie 3 lat od dnia dostawy. Zapis ten jest bardzo nieprecyzyjny. Przypominamy, że na Zamawiającym spoczywa obowiązek jasnego i precyzyjnego określenia przedmiotu zamówienia, a co za tym idzie, wykorzystania do jego opisanego standardowych określeń technicznych, które są zwykle używane w danej dziedzinie, zrozumiałych dla wszystkich osób trudniących się działalnością w danej branży. Utrzymanie powyższego zapisu mogłoby narazić Zamawiającego na zarzut niegospodarnego zarządzania środkami publicznymi.

Wnioskujemy o wykreślenie zapisu:

Urządzenie dostarczone z najbogatszym pakietem funkcjonalności (subskrypcji) oferowanym przez producenta w dniu dostawy, obowiązującym w okresie 3 lat od dnia dostawy.

**Odp. 15.**

W trosce o gospodarkowanie środkami publicznymi, Zamawiający w chwili zakupu urządzenia chce mieć pewność, że zostanie ono dostarczone wraz z wszystkimi niezbędnymi dla niego funkcjonalnościami, tym samym chce się ustrzec sytuacji, w której Wykonawca dostarczy urządzenie, którego użytkowanie z wykorzystaniem pełni jego funkcji wymagać będzie zakupu dodatkowych licencji, a tym samym dodatkowego wydatkowania środków publicznych. Na potrzeby odpowiedzi na pytanie Wykonawcy, Zamawiający przedstawia minimalną ilość podstawowych funkcjonalności, które muszą być zawarte w pakiecie subskrypcji dostarczonym wraz z urządzeniem na okres 3 lat: Firewall + IDS/IPS, IPSec & SSL VPN, ochrona antywirusowa, filtr URL, ochrona antyspamowa, kontrola aplikacji.

W związku z powyższym, Zamawiający dokonał zmiany zapisu zał. 1.1.A z "Urządzenie dostarczone z najbogatszym pakietem funkcjonalności (subskrypcji) oferowanym przez producenta w dniu dostawy, obowiązującym w okresie 3 lat od dnia dostawy." na:

"Urządzenie dostarczone z pakietem funkcjonalności (subskrypcji) oferowanym przez producenta, obowiązującym w okresie 3 lat od dnia dostawy zawierającym minimum funkcjonalności: Firewall + IDS/IPS, IPSec & SSL VPN, zaawansowany antywirus, filtr URL, ochrona antyspamowa, kontrola aplikacji, wsparcie certyfikowanego partnera."

**Pytanie 16** - W oświadczeniu na str. 3 Załącznika nr 1.1.A do SIWZ znajduje się zapis:

Dostarczone urządzenie oraz dostępny do niego pakiet funkcjonalności zapewni Zamawiającemu zgodność z wymaganiami przepisów Unii Europejskiej „General Data Protection – GDPR” (w Polsce RODO).

Zapis ten jest niemożliwy do spełnienia poprzez zakup i wdrożenie Urządzenia UTM/NextGen Firewall. Informujemy Zamawiającego, że nie istnieje takie rozwiązanie teleinformatyczne, które zapewni Zamawiającemu zgodność z wymaganiami przepisów Unii Europejskiej „General Data Protection – GDPR” (w Polsce RODO).

Utrzymanie powyższego zapisu spowoduje, że postępowanie przetargowe będzie obciążone wadą prawną niemożliwą do usunięcia.

Wnioskujemy o wykreślenie zapisu:

Dostarczone urządzenie oraz dostępny do niego pakiet funkcjonalności zapewni Zamawiającemu zgodność z wymaganiami przepisów Unii Europejskiej „General Data Protection – GDPR” (w

Polsce RODO).

**Odp. 16** – Zamawiający zdaje sobie sprawę, że zakup i wdrożenie urządzenia UTM/NextGenFW nie zaspokoi wszystkich wymagań nakładanych przez zapisy GDPR/RODO, intencją Zamawiającego było tylko zwrócenie Wykonawcom uwagi na funkcjonalności opisane w RODO, które mogą być zaimplementowane w tego typu sprzęcie. Aby uniknąć jednak niejasności w tym zakresie, Zamawiający usuwa z zał. 1.1.A zapis: "Dostarczone urządzenie oraz dostępny do niego pakiet funkcjonalności zapewni Zamawiającemu zgodność z wymaganiami przepisów Unii Europejskiej „General Data Protection – GDPR” (w Polsce RODO)".

**Pytanie 17** – Dogłębna analiza wymogów opisujących przez Zamawiającego przedmiot zamówienia (Załącznik nr 1.1.A do SIWZ) nie pozwala złożyć oferty w postępowaniu na rozwiązanie inne niż Sophos UMT. - Wnioskujemy o dopisanie:

1. Lub równoważnego certyfikatu dotyczącego VPN do:

Urządzenie ma posiadać certyfikat ICSA IPsec VPN;

**Odp. 17** - Zamawiający dokonuje zmiany w/w zapisu na:

Urządzenie ma posiadać certyfikat ICSA IPsec VPN lub certyfikaty równoważne;

**Pytanie 18** - Wnioskujemy o wykreślenie:

1.L2TP z: "Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów min: IPsec, SSL, L2TP;"

**Odp.** - Zamawiający dokonuje zmiany zapisu na: "Obsługa połączenia VPN client-to-site z wykorzystaniem protokołów min: IPsec, SSL;"

2. z jednoczesną obsługą co najmniej 3 serwerów DHCP z: "Funkcjonalność pracy w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP"

**Odp.** Zamawiający dokonuje zmiany zapisu na: "Funkcjonalność pracy w trybie DHCP Relay;"

**Pytanie 19.** Wnioskujemy o wykreślenie:

1. Obsługa Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web;

**Odp.** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

2. Antywirus musi mieć możliwość przeprowadzania kwarantanny poczty e-mail;

**Odp.** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

3. Antyspam oparty na technologii RPD - Recurrent Pattern Detection;

**Odp.** Zamawiający usuwa z zał. 1.1.A w/w zapis;

4. System musi mieć możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy;

**Odp.** Zamawiający nie zmienia zapisów zał. 1.1.A w tym zakresie;

5. Agent instalowany na końcówkach użytkowników z podpunktami

**Odp.** W/w zapisy dotyczą oprogramowania klienta, którego dostawa nie jest wymagana obligatoryjnie, jest wymaganiem opcjonalnym/dodatkowym, punktowanym dodatkowo w ramach dostarczenia aplikacji agenta przeznaczonego do instalowania na stacjach roboczych i współpracującego z urządzeniem. W związku z tym, Wykonawca może dostarczyć urządzenie, bez licencji agenta o którym mowa powyżej. Zamawiający nie dokonuje zmian w zał. 1.1.A w tym zakresie.

6. Możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty);

**Odp.**- Zamawiający dokonuje usunięcia w/w zapisów z zał. 1.1.A

7. Automatyzacja generowania raportów (według harmonogramu – codziennie, tygodniowo) wraz z możliwością ich wysyłania pocztą e-mail;

**Odp.** Zamawiający dokonuje zmiany w/w zapisu na zał. 1.1.A na: "Generowanie raportów wraz z możliwością ich wysyłania pocztą e-mail, lub przygotowanie linków URL generujących żądany



raport według zaprogramowanych kryteriów."

8. Możliwość kontroli dostępu do dzienników i raportów opartego na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom;

**Odp.** Zamawiający usuwa z zał. 1.1.A w/w zapis;

9. Możliwość anonimizacji danych użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów.

**Odp.** Zamawiający usuwa z zał. 1.1.A w/w zapis;

**Pytanie 20** - Obsługa statycznego i dynamicznego (routowane) połączenia VPN do > dostawców chmury obliczeniowej (AWS i MS Azure). Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 20** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

**Pytanie 21** - Urządzenie ma posiadać certyfikat ICSA IPSec VPN, Czy zamawiający dopuszcza rozwiązanie nie posiadające certyfikatu ICSA dla IPSec ale posiadające certyfikat równoważne?

**Odp. 21** - Zamawiający dokonuje zmiany w/w zapisu na:

Urządzenie ma posiadać certyfikat ICSA IPSec VPN lub certyfikaty równoważne;

**Pytanie 22** - Antywirus musi mieć możliwość przeprowadzania kwarantanny poczty e-mail, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 22** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

**Pytanie 23** - Możliwość zablokowania oprogramowania typu ransomware uruchomionego na stacjach roboczych i serwerach, Czy zamawiający potwierdza że ten wymóg jest wymogiem opcjonalnym/dodatkowym, punktowanym dodatkowo w ramach dostarczenia aplikacji do instalowania na stacjach roboczych?

**Odp. 23** - Tak, jest to wymóg opcjonalny/dodatkowy, punktowany dodatkowo w ramach dostarczenia aplikacji do instalowania na stacjach roboczych.

**Pytanie 24** - Antyspam oparty na technologii RPD - Recurrent Pattern Detection, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 24** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

**Pytanie 25** - Możliwość blokowania spamu opartego na obrazach graficznych, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 25** - Zamawiający usuwa z zał. 1.1.A w/w zapis;

**Pytanie 26.** - System musi mieć możliwość blokowania poczty zawierającej podejrzone załączniki do czasu zakończenia ich analizy, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 26** - **Odp.** Zamawiający nie zmienia zapisów zał. 1.1.A w tym zakresie;

**Pytanie 27.** - Agent instalowany na końcówkach użytkowników z podpunktami, Czy zamawiający potwierdza że ten wymóg jest wymogiem opcjonalnym/dodatkowym, punktowanym dodatkowo ?

**Odp. 27** - Tak, jest to wymóg opcjonalny/dodatkowy, punktowany dodatkowo w ramach dostarczenia aplikacji do instalowania na stacjach roboczych.

**Pytanie 28** - Automatycznego dopasowania rozdzielczości i czytelności interfejsu WWW podczas pracy na różnych urządzeniach, Czy zamawiający dopuszcza rozwiązanie, którego interfejs administracyjny jest zgodny z przeglądarkami IE oraz FireFox a więc jego zgodność z różnymi urządzeniami nie jest wymagana?

**Odp. 28** - Tak, Zamawiający dopuszcza takie rozwiązanie.

**Pytanie 29.** Możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty);

**Odp. 29 -** Zamawiający wyraża zgodę na dostawę urządzenia nie spełniającego w/w wymagań i w związku z tym dokonuje usunięcia w/w zapisów z zał. 1.1.A.

**Pytanie 30.** System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 30 -** W/w zapis dotyczy funkcjonalności agenta, jest to wymóg opcjonalny/dodatkowy, punktowany dodatkowo w ramach dostarczenia aplikacji do instalowania na stacjach roboczych i w związku z tym nie jest ona wymagana.

**Pytanie 31.** Automatyzacja generowania raportów (według harmonogramu – codziennie, tygodniowo) wraz z możliwością ich wysyłania pocztą e-mail, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności? Ale umożliwia przygotowanie linków URL generujących żądany raport według zaprogramowanych kryteriów.

**Odp. 31.** Zamawiający dokonuje zmiany w/w zapisu na zał. 1.1.A na: "Generowanie raportów wraz z możliwością ich wysyłania pocztą e-mail, lub przygotowanie linków URL generujących żądany raport według zaprogramowanych kryteriów."

**Pytanie 32 -** Możliwość kontroli dostępu do dzienników i raportów opartego na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 32.** Zamawiający usuwa z zał. 1.1.A w/w zapis.

**Pytanie 33 -** Możliwość anonimizacji danych użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów, Czy zamawiający dopuszcza rozwiązanie nie posiadające takiej funkcjonalności?

**Odp. 33 -** Zamawiający usuwa z zał. 1.1.A w/w zapis.

**Pytanie 34 -** Ilość rozpoznawanych aplikacji nie mniejsza niż 1500, Czy zamawiający dopuszcza rozwiązanie w którym sygnatury aplikacyjne tworzone są z uwzględnieniem typu aplikacji a nie pojedynczej aplikacji? Dzięki takiemu podejściu chociaż urządzenie ma mniej niż wymagane 1500 rozpoznaje znacznie więcej aplikacji na podstawie ich typu.

**Odp. 34 -** Zamawiający usuwa z zał. 1.1.A w/w zapis.

**W związku z pytaniami Wykonawców, Zamawiający dokonał zmian w specyfikacji dot. Urządzenia UTM/NextGen Firewall – ZAŁ. 1.1.A – w załączeniu.**

**Część 2 -** przedłużenie licencji oprogramowania antywirusowego ESET na okres minimum 3 lat lub dostawę nowego oprogramowania antywirusowego na okres minimum 3 lat

Czy zamawiający dopuszcza aby rozwiązanie nie spełniało wymagań z Załącznik Nr 1.2.A do SIWZ:

**Pytanie 1 -** Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera), przy czym każde zadanie może być uruchomione z własnymi ustawieniami, możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur;

**Odp. 1 -** Zamawiający usuwa z zał. 1.2.A powyższy zapis;

**Pytanie 2** - Możliwość tworzenia hierarchii serwerów zarządzających (serwer pojedynczy, lub serwer główny + serwery podrzędne w różnych podsięciach), z możliwością pobierania aktualizacji oprogramowania, definicji oraz polityk bezpieczeństwa z serwera głównego i rozsyłania na serwery podrzędne, lub zastosowania jednego centralnego serwera zarządzania bez względu na wielkość sieci – w zależności od wyboru Administratora;

**Odp. 2 - Zamawiajcy dokonuje zmiany zapisu na:**

Możliwość instalacji serwera zarządzającego w sieci lokalnej Zamawiającego, obsługującego minimum rolę: serwera bazodanowego, serwer aktualizacji, serwer komunikacji, konsola zarządzająca;

**Pytanie 3** - Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu;

**Odp. 3 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 4** - Mechanizm skanowania heurystycznego z wyborem stopnia jego zaawansowania (pasywne metody heurystyczne, lub aktywne – zaawansowane z elementami sztucznej inteligencji) możliwością włączenia jednego lub obu trybów, wyboru zaawansowania poziomu leczenia infekcji oraz profilu skanowania plików;

**Odp. 4 - Zamawiajcy dokonuje zmiany zapisu na:**

Obsługa mechanizmu skanowania heurystycznego;

**Pytanie 5** - Skanowanie i oczyszczanie poczty elektronicznej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego) wraz z możliwością dołączenia opcjonalnego komunikatu o wykonaniu skanowania do oryginalnej wiadomości pocztowej;

**Odp. 5 - Zamawiajcy dokonuje zmiany zapisu na:**

Skanowanie i oczyszczanie poczty elektronicznej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego);

**Pytanie 6** - Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera, fakt ten musi być potwierdzony odpowiednim komunikatem interfejsu aplikacji, przy czym ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera;

**Odp. 6 - Zamawiajcy dokonuje zmiany zapisu na:**

Możliwość tymczasowego wyłączenia ochrony do ponownego uruchomienia komputera, lub włączenia ochrony przez użytkownika;

**Pytanie 7** - Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS, przy czym program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe a administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego;

**Odp. 7 - Zamawiajcy dokonuje zmiany zapisu na:**

Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów, przy czym program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe;

**Pytanie 8** - Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta;

**Odp. 8 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 9** - Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego



reputacji bezpośrednio z poziomu menu kontekstowego;  
**Odp. 9 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 10** - Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model oraz co najmniej uprawnień: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia;

**Odp. 10 -Zamawiający dokonuje zmiany zapisu na:**

Funkcja skanowania i blokowania nośników wymiennych z możliwością określenia poziomu dostępu do urządzeń;

**Pytanie 11** - Program musi być wyposażony w moduł HIPS działający w jednym z pięciu trybów: 1) tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, 2) tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, 3) tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, 4) tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach. 5) tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach;

**Odp. 11 - Zamawiający dokonuje zmiany zapisu na:**

Program musi być wyposażony w moduł HIPS ;

**Pytanie 12** - Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego, na etapie tworzenia reguł dla modułu HIPS musi istnieć możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól;

**Odp. 12 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 13** - Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach;

**Odp. 13 - Zamawiający dokonuje zmiany zapisu na:**

Program ma umożliwić sprawdzenie podstawowych informacji na temat stacji, na której został zainstalowany, w tym przynajmniej jej adres IP oraz wersję systemu operacyjnego;

**Pytanie 14** - System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line);

**Odp. 14 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 15** - Aplikacja musi wspierać skanowanie magazynu Hyper-V;

**Odp. 15 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 16** - Opcjonalnie oprócz gotowej maszyny wirtualnej, administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta;

**Odp. 16 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 17** - Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny, przy czym serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem

centralnym, musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym i musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów;

**Odp. 17 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 18** - Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis, musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika, musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego;

**Odp. 18 - Zamawiający dokonuje zmiany zapisu na:**

Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów serwera centralnego zarządzania do zarządzania stacjami roboczymi;

**Pytanie 19** - Serwer musi umożliwiać podział wykonywanych zadań na dwie grupy: zadania serwera (instalacji agenta, generowania raportów oraz synchronizacji grup) oraz zadania klienta wykonywane za pośrednictwem agenta na stacji roboczej, który musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji;

**Odp. 19 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 20** - Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów - dynamiczne tworzone na podstawie szablonu określającego warunki j, np.: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, itp;

**Odp. 20 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 21** - Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta, przy czym opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku;

**Odp. 21 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 22** - Musi istnieć możliwość tymczasowego wstrzymania polityk przesłanych z poziomu serwera zdalnej administracji, ma to umożliwić lokalną zmianę ustawień programu na stacji końcowej, przy czym wstrzymanie polityki musi być realizowane tylko przez określony czas, po którym automatycznie zostają przywrócone dotychczasowe ustawienia (na 10 min, 30 min, 1 godzinę i 4 godziny), wstrzymanie polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika;

**Odp. 22 - Zamawiający dokonuje zmiany zapisu na:**

Musi istnieć możliwość tymczasowego wstrzymania polityk przesłanych z poziomu serwera zdalnego;

**Pytanie 23** - Możliwość zdefiniowania w harmonogramie zadań sprawdzających rodzaj zasilania na którym pracuje komputer (sieć/bateria) i zawieszających dalsze wykonywanie określonych zadań jeśli komputer pracuje na zasilaniu bateryjnym;

**Odp. 23 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;**

**Pytanie 24** - Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera), przy czym każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (metody skanowania, skanowane obiekty, wykonywane czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

Odp. 24 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;

Pytanie 25 - Administrator powinien mieć możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik;

Odp. 25 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;

Pytanie 26 - Możliwość identyfikacji licencji wykorzystanej do aktywacji programu, lub ukrycia tej informacji;

Odp. 26 - Zamawiający dokonuje zmiany zapisu na:

Możliwość identyfikacji licencji wykorzystanej do aktywacji programu;

Pytanie 27 - Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych;

Odp. 27 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;

Pytanie 28 - Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie;

Odp. 28 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;

Pytanie 29 - Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli administracyjnej;

Odp. 29 - Zamawiający usuwa z zał. 1.2.A powyższy zapis;

W związku z pytaniami Wykonawców, Zamawiający dokonał zmian w specyfikacji dot. przedłużenia licencji oprogramowania antywirusowego ESET na okres minimum 3 lat lub dostawę nowego oprogramowania antywirusowego na okres minimum 3 lat – ZAŁ. 1.2.A – w załączeniu.

Wszelkie dokonane zmiany znajdują się w zmienionych załącznikach 1.1.A do SIWZ dla części 1 postępowania oraz 1.2.A do SIWZ dla części 2 postępowania.

Termin oraz miejsce składania i otwarcia ofert pozostają bez zmian.

Z upoważnienia Dyrektora  
KZGM w Katowicach

*Wioletta Kotłowiec*

**Załączniki:**

- formularz asortymentowo – cenowy zał nr 1.1.A do SIWZ;
- formularz asortymentowo – cenowy zał nr 1.2.A do SIWZ;

Kopia: NZ - a/a

Prowadząca sprawę: Jacek Świerczyński

Dział Organizacji Przetargów

032 416 31 50



Komunalny Zakład Gospodarki Mieszkaniowej w Katowicach

ul. Grażyńskiego 5  
40-126 Katowice  
skr. poczt. 334

tel.: 32 258 20 21 do 25  
faks: 32 258 20 25  
NIP 634 269 76 80

www: <http://kzgm.katowice.pl>  
email: [poczta@kzgm.katowice.pl](mailto:poczta@kzgm.katowice.pl)  
REGON 241031620

