Załącznik nr 1 – Szczegółowy opis przedmiotu zamówienia do zapytania ofertowego z dnia 10.04.2017

Przedmiotem zamówienia jest stworzenie systemu do metaanalizy statystycznej i interpretacji wyników badań tj:

1. Dostęp on-line do w pełni zintegrowanej bazy do przeprowadzenia analiz genetycznych NGS (analizy bioinformatycznej, określenie jakości, wizualizacja, przechowywanie plików pacjentów przez okres minimum 5 lat).
2. System ochrony antywirusowej z zaporą ogniową dla stacji roboczych,
3. Serwer plików NAS, 1 sztuka,
4. Dyski twarde, 8 sztuk,
5. Szafa dystrybucyjna 42U 19" 80cmx80cm (szer. x głęb.),
6. Serwer, 2 sztuki.

Specyfikacja dla każdego z w/w produktów:

Ad 1.

Wymagania dotyczące dostępu on-line do w pełni zintegrowanej bazy do przeprowadzenia analiz genetycznych NGS.

Założenia:

1. Wymagania dla bazy- certyfikat ISO.

2. Wymagane jest przeprowadzenie standardowego programu walidacyjnego obejmującego analizę dwóch sekwencjonowań NGS (ang. – Next Generation Sequencing) i raport, analizę jakości, konsultacje, trening, raport z wydajności/jakości analiz, certyfikat jakości. W ramach walidacji wymagane jest dostarczenie min 3 referencyjnych próbek.

Ad 2.

Wymagania dotyczące systemu ochrony antywirusowej z zaporą ogniową dla stacji roboczych.

Istotne cechy oprogramowania :

1.Ochrona antywirusowa stacji roboczych :
- Microsoft Windows XP with SP3 (32-bit)

- Microsoft Windows Vista (32-bit i 64-bit)

- Microsoft Windows Vista SP1 lub nowszy (32-bit i 64-bit)

- Microsoft Windows 7 (32-bit i 64-bit)

- Microsoft Windows 7 SP1 lub nowszy (32-bit i 64-bit)

- Microsoft Windows 8 (32-bit i 64-bit)

2.Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z portalu zarządzającego dostępnego on-line przez przeglądarkę internetową.
3.Możliwość podłączenia stacji do zdalnego portalu zarządzającego niezależnie na kilku wybranych stacjach.
4.Polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą.
5.Sprzedający musi posiadać niezależny od klienta końcowego dostęp do komputerów klienta końcowego podpiętych do portalu zarządzającego

Wymagania dotyczące technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
4. Skanowanie poczty e-mail pod kątem niepożądanych wiadomości (ochrona anty-spamowa) ; ochrona przed phishingiem.
5. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
6. Możliwość wywołania skanowania na żądanie z poziomu portalu zarządzającego dla pojedynczego lub wielu komputerów lub lokalnie przez określonego klienta.
7. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
8. Brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
9. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
10. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
11. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
12. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.
13. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
14. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
18. Automatyczne uruchamianie procedur naprawczych.
19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
20. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.
21. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
22. Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów. W programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP. Obsługuje m.in. MS Outlook Express, MS Outlook, Mozilla, Eudora, Netscape Mail.
23. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
24. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie gdy stacja robocza posiada stare sygnatury antywirusowe.
25. Ochrona podczas przeglądania sieci Internet przy pomocy – integracja z przeglądarką internetową Internet Explorer 6 oraz Mozilla 2 (lub wyższe wersje).
26. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
27. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN.

28. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
29. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
30. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
31. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7.
32. Moduł służący aktualizacji oprogramowania firm trzecich wraz z aktualizacjami systemu Windows.

Wymagania dotyczące systemu zarządzania centralnego:

1. Portal zarządzający wraz z edytorem profilów bezpieczeństwa dostępny w języku polskim,
2. Portal zarządzający umożliwia pobranie plików instalacyjnych stacji roboczych oraz stacji serwerowych oraz pobranie narzędzia instalacji zdalnej,
3. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nową wersję,
4. Administracja, konfiguracja profilów bezpieczeństwa i monitorowanie stacji roboczych i serwerów plików za pomocą portalu zarządzającego,
5. Komunikacja pomiędzy portalem zarządzającym, a stacjami roboczymi podpisywana jest po instalacji oprogramowania oraz bazuje na podstawie wpisywanego podczas procesu instalacji klucza instalacyjnego,
6. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, portal zarządzający pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta,
7. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów,
8. Portal zarządzający musi umożliwiać usuwanie klientów ze swoich grup z całkowitym zachowaniem ustawień oraz przypisanych profili bezpieczeństwa,
9. Tworzenie grup , zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach,
10. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych i w celu uniemożliwienia ich modyfikacji przez użytkowników,
11. Portal zarządzający musi mieć możliwość wysłania żądania aktualizacji stanu stacji roboczej w celu odświeżenia informacji w portalu zarządzającym,
12. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania,
13. Dane powinny być przesyłane do portalu zarządzającego podczas kolejnego połączenia,
14. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji,
15. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje),
16. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe,
17. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”,
18. Portal zarządzający musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa,
19. Portal zarządzający musi pozwalać na określenie wykluczonych obszarów ze skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe,
20. Program musi pozwalać na określenie typów skanowanych plików

Ad 3 .

Wymagania dotyczące serweru plików NAS – 1 sztuka

Założenia :

1. Serwer plików ma być w wyposażony w czterordzeniowy procesor typu Intel Atom C2538 Quad Core 2,4 Ghz lub równoważny.
2. Serwer ma mieć wbudowane 2GB DDR3 pamięci RAM z możliwością rozszerzenia do 6GB.
3. Wewnętrzny dysk HDD/SSD – możliwość montażu 8 x 3,5" lub 2,5" SATA (II) (dyski twarde nie wchodzą w skład zestawu).
4. Serwer musi umożliwiać wymianę dysków podczas pracy.
5. Serwer musi być wyposażony w minimum 4x Gigabit LAN z obsługą agregacji łączy (link aggregation).
6. Serwer musi obsługiwać następujące protokoły sieciowe: CIFS, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
7. Serwer musi wspierać systemy plików EXT4, EXT3, FAT, NTFS, HFS+
8. Maksymalny rozmiar systemu plików: 108 TB, maks. liczba wolumenów wewnętrznych: 512, maksymalna liczba iSCSI Target: 32, maks. liczba iSCSI LUN: 256, obsługa klonowania i migawek RAID, obsługiwany typ RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10

Ad 4.

Wymagania dotyczące dysków twardych – 8 sztuk

Założenia:

1. Osiem dysków twardych 3,5" o pojemności 6TB przeznaczonych do serwerów NAS – WD RED 6TB lub równoważne.

Ad 5.

Wymagania dotyczące szafy dystrybucyjnej 42U 19" 80cmx80cm (szer. x głęb.)

Założenia:

1. Szafa musi umożliwiać montaż urządzeń aktywnych o rozstawie 19".
2. Wysokość użytkowa szafy 42U.
3. Jednostka "U" określa wysokość urządzeń aktywnych o szerokości montażowej 19 cali (48.26cm) przeznaczonych do montażu w szafach typu 'rack'. Jedna jednostka „U" (ang. „Rack Unit" wynosi 1,75 cala (44,45mm)
4. Szafa musi umożliwiać montaż urządzeń aktywnych na słupkach nośnych (2 pary: przód i tył).
5. Szafa musi posiadać: przednie drzwi przezroczyste (dopuszcza się przyciemniane) zamykane na przynajmniej jeden zamek trzypunktowy z kluczem; konieczna możliwość montażu drzwi jako lewo i prawo stronne. Szyba spełniająca normy bezpieczeństwa.
6. Szafa musi posiadać ściany boczne i tylna zdejmowane.
7. Szafa musi posiadać listwę uziemiającą i linki elastyczne (zerujące różnicę potencjału) łączące
   ściany i drzwi szafy.
8. Szafa musi posiadać nóżki umożliwiające regulację pionu i poziomu szafy.
9. Szafa musi posiadać możliwość montażu panelu wentylacyjnego na górnej ścianie (suficie) w fabrycznie dedykowanych miejscach.
10. Każda szafa musi posiadać dedykowany dla niej dachowy system wentylacyjny składający się z minimum 4 wentylatorów.
11. Powłoka lakiernicza: farba proszkowa.
12. Szafa musi posiadać prefabrykowane otwory na wypuszczenie okablowania zasilającego i sieciowego.
13. Zamawiający dopuszcza szafę do samodzielnego montażu.
14. Szafa wyposażona w min. 3 półki.
15. Minimalna wartość dopuszczalnego obciążenia szafy: 750 kg.

Ad 6.

Wymagania dotyczące serwerów – 2 sztuki

Założenia:

Serwery (2 sztuki) o parametrach nie gorszych niż:

1. Procesor: Intel Xeon X5675 / 3.06 GHz 6,40GT/s
2. Typ Procesora: 2-CPU / XEON DP
3. Cache: 12 MB
4. Taktowanie procesora: 3.06 GHz
5. Liczba zainstalowanych procesorów: 2 sztuki
6. Maks. obsługiwana liczba procesorów: 2 sztuki
7. Typ pamięci : DDR3 RDIMM ECC
8. Maksymalna wspierana pojemność: 384 GB
9. Zainstalowana pamięć RAM: 96 GB (12x 8 GB)
10. Moc wyjściowa: 750 Watt, Hot Plug
11. Zasilanie nadmiarowe: TAK
12. Ilość zainstalowanych zasilaczy: 2
13. Pamięć wideo: 64 MB standard
14. Poziom RAID: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
15. Typ kontrolera: S-ATA 6GB/s – zintegrowany
16. Typ intefejsu kontrolera: 3Gb/s SATA
17. Ilość kanałów: 8
18. Twardy dysk: SATA HDD
19. Pojemność dysków: 2TB
20. Typ interfejsu: SATA
21. Ilość zainstalowanych dysków: 2
22. Prędkość obrotów: -
23. Gniazdo procesora: LGA1366 Socket
24. Ilość gniazd pamięci RAM: 12x DDR3 PC3-10600/8500, ECC (12 już w użyciu)
25. Kontroler Ethernet:-
26. Zainstalowane karty sieciowe: 2xHP NC365T (4-port Ethernet), 2 x HP QLOGIC FTLF8524E2KNL (4GB PCIe Dual Port)
27. Kieszenie na dyski: SATA
28. Obudowa: Rack 2U
29. Wymiary: 8.59 x 44.55 x 69.22 cm
30. Waga: 21.45 kg / 27.27 kg
31. Obsługiwane systemy operacyjne: Windows Server 2012 R2, Linux
32. System operacyjny: Brak