Zadanie nr 1 - Dostawy zestawów komputerowych biurowych

OPIS PRZEDMIOTU ZAMÓWIENIA (po uwzględnieniu udzielonych odpowiedzi na pytania)

**Załącznik nr 2a do SIWZ**

**Opis przedmiotu zamówienia**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne asortymentu** |
|  | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ oraz model oferowanego komputera. |
|  | Obudowa | Małogabarytowa metalowa obudowa przystosowana do pracy w pionieObudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa otwierana bez użycia narzędzi umożliwiająca dostęp do pamięci masowej, pamięci ram.Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem katalogowym PN, numerem seryjnym. |
|  | Chipset | Dostosowany do zaoferowanego procesora, lub równoważny |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Wyposażona w 2 sloty na pamięć RAM DDR4 |
|  | Procesor | Procesor osiągający w teście PassMark CPU Mark wynik min. 5700 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net w okresie od dnia ukazania się ogłoszenia oraz nie później niż jeden dzień przed składaniem oferty. |
|  | Pamięć operacyjna | Min. 8GB RAM, 2400MHz DDR4. Pamięć pracująca w trybie dual-channel.Możliwość rozbudowy do 32 GB.  |
|  | Dysk twardy | Min. 256GB SSD zamontowany fabrycznie, zawierający partycję RECOVERY umożliwiającą odtworzenie po awarii systemu operacyjnego, fabrycznie zainstalowanego na komputerze.  |
|  | Napęd optyczny | Zintegrowna nagrywarka DVD z komputerem  |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. |
|  | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  |
|  | Karta sieciowa | 10/100/1000 – złącze RJ45 |
|  | Porty/złącza | Wbudowane porty z przodu obudowy:2 x USB 3.0 1 z czego jeden umożliwiający szybkie ładowanie podłączonego urządzenia nawet przy wyłączonym komputerze1 x port Combo umożliwiający podłączenie słuchawek wraz z mikrofonemlub port mikrofonowy lub port umożliwiający podłączenie słuchawekWbudowane porty z tyłu obudowy:- 1 x DP, - 2 x USB 3.0 - 2 x USB 2.0- 1 x port sieciowy RJ-45, - 1 x Serial PortWymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z płytą główną. |
|  | Klawiatura/mysz | Klawiatura przewodowa w układzie US lub EU, USB, kabel min 1,5mMysz przewodowa (optyczna lub laserowa) 3 przyciskowa (scroll), USB, kabel min. 1,5m |
|  | Zasilacz | Energooszczędny zasilacz o mocy nie większej niż 280W oraz sprawności na poziomie min. 85%. wraz z kablem zasilającym - złącza: Hybrydowe typu C/E/F męskie - IEC C13 ,min. 1.8m, kolor czarny |
|  | System operacyjny | Zainstalowany/preinstalowany nowy, nieaktywowany nigdy wcześniej na innym urządzeniu, system operacyjny: Oryginalny Windows 10 Pro. PL 64-bit z licencją lub równoważny.Parametry równoważności:* pełna integracja z systemami IBM Lotus Notes, SWOP, Płatnik;
* pełna obsługa ActiveX;
* dostępne dwa rodzaje graficznego interfejsu użytkownika, w tym: - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

- dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych;* możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
* wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
* wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
* system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);
* zgodny z posiadanym przez zamawiającego oprogramowaniem MS Office 2007/2010/2013/2016, oprogramowaniem IBM Tivoli Endpoint Manager for Lifecycle Management (wraz z instalacją agenta IBM TEM);
* oprogramowanie powinno umożliwiać zainstalowanie oprogramowania

(Kies, Active Sync lub Centrum obsługi urządzeń z systemem WindowsMobile, PC Suitę lub Nokia Suitę, Zune, iTunes) umożliwiającego pełną synchronizację i zgrywanie kontaktów i danych między używanymi przez Zamawiającego telefonami komórkowymi (Nokia, Iphone, Samsung, Telefunken) oraz komputerem.* oprogramowanie powinno zawierać certyfikat autentyczności lub unikalny kod aktywacyjny;

Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji Microsoft Windows 10 |
|  | BIOS  | BIOS zgodny ze specyfikacją UEFI- Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera,- MAC Adres karty sieciowej,- wersja Biosu wraz z datą produkcji,- zainstalowanym procesorze, jego taktowaniu - ilości pamięci RAM wraz z taktowaniem,- napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego)Możliwość z poziomu Bios:- wyłączenia kontrolera selektywnego (pojedynczego) portów SATA,- konfiguracji kontrolera SATA: AHCI - wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE- ustawienia hasła: administratora, Power-On, HDD,- alertowania zmiany konfiguracji sprzętowej komputera - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - załadowania optymalnych ustawień Bios- obsługa Bios za pomocą klawiatury - obsługa Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
|  | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:wykonanie testu pamięci RAM test dysku twardegoWizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
|  | Certyfikaty i standardy | * Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)
* Deklaracja zgodności CE (załączyć do oferty)
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
 |
|  | Waga/rozmiary urządzenia wraz z napędem optycznym. | Waga urządzenia max. 8kgSuma wymiarów nie może przekraczać: 900mm |
|  | Bezpieczeństwo i zdalne zarządzanie | * Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy
* Moduł TPM 2.0
 |
|  | Oprogramowanie | Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników.  |
|  | Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site).W przypadku awarii dysku twardego dysk uszkodzony pozostaje u ZamawiającegoW przypadku potrzeby przekazania sprzętu do serwisu poza miejscem użytkowania, zostanie on wysłany bez dysku twardego.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.- możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne monitora**  |
| Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9) |
| Rozmiar plamki | 0,275 mm |
| Jasność | 250 cd/m2 |
| Kontrast | Typowy 1000:1 |
| Kąty widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy | max. 8 ms (Gray to Gray) |
| Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
| Częstotliwość odświeżania poziomego | 30 – 80 kHz |
| Częstotliwość odświeżania pionowego | 56-60 Hz |
| Zyżycie energii | Normalne działanie 22W (typowe), 43W(maksymalne), tryb wyłączenia aktywności mniej niż 0,3W |
| Powłoka powierzchni ekranu | Antyodblaskowa utwardzona |
| Podświetlenie | System podświetlenia LED |
| Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Lock - gniazdo zabezpieczenia przed kradzieżą. |
| Waga bez podstawy | Maksymalnie 3,30kg |
| Waga z podstawą + kable | Maksymalnie 5,70kg |
| Wymiary bez podstawy | Wysokość : max. 340 mmSzerokość : max. 570 mmGłębokość : max. 64 mm |
| Wymiary z podstawą | Wysokość : max. 430 mmSzerokość : max. 570 mmGłębokość : max. 230 mm |
| Zakres regulacji Tilt | Wymagany, od -5 do +21 lub min. regulacja 26 stopni |
| Kolor obudowy | Czarny |
| Głośniki | Wbudowane lub dedykowane przez producenta monitora, głośniki doczepiane lub jako listwa dźwiękowa o parametrach nie gorszych niż :Całkowita moc: 2,5 W Pasmo przenoszenia: od 140 Hz do 20 KHz |
| Złącze  | 1x D-Sub, 1x DisplayPort |
| Gwarancja | 3 lata na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczegoFirma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty.Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |
| Certyfikaty | TCO 7.0, ISO 13406-2 lub ISO 9241Wymagane dokumenty dołączyć do oferty dodatkowo potwierdzone przez producenta sprzętu oświadczeniem lub podpisane przez osobę upoważnioną/prokurenta do reprezentowania producenta sprzętu.  |
| Inne | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm- w zestawie kabel zasilający złącza: Hybrydowe typu C/E/F męskie - IEC C13 ,min. 1.8m, kolor czarny oraz - kabel DSUB min. 1.8m- kabel DisplayPort – DisplayPort, min. 1.8 m- kabel DisplayPort – HDMI, min. 1.8 m |

Zadanie nr 2 – Dostawy zestawów komputerowych graficznych

OPIS PRZEDMIOTU ZAMÓWIENIA (po uwzględnieniu udzielonych odpowiedzi na pytania)

**Załącznik nr 2b do SIWZ**

**Opis przedmiotu zamówienia**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Komputer – stacja graficzna | Komputer będzie wykorzystywany dla potrzeb aplikacji graficznych oraz monitorujących dlatego zaoferowany sprzęt musi być przystosowany do pracy ciągłej.  |
|  | Typ | W ofercie należy podać nazwę producenta, typ oraz model oferowanego urządzenia. |
|  | Obudowa | Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu.Obudowa wyposażona w min. 4 kieszenie musi umożliwiać (oprócz napędu DVD) montaż urządzeń min.:-1x5,25” (do wykorzystania przez zamawiającego) - 2 x 3,5” wewnętrzne (np. do montażu czytnika kart)Obudowa musi umożliwiać beznarzędziowe otwarcie, demontaż dysków twardych (3,5”), napędu optycznego oraz kart rozszerzeń. Wyklucza się użycie jakichkolwiek śrub.Obudowa musi być wyposażona w czujnik otwarcia obudowy oraz zamek Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem konfiguracji oraz numerem seryjnym |
|  | Chipset | Dedykowany rozwiązaniom serwerowym lub stacji graficznych chipset lub równoważny wspierający system kodowania korekcyjnego ECC (ang. Error Correction Code)  |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji).Wyposażona w min. 6 złącz SATA 3.0 (6Gb/s) z czego jedno złącze dedykowane do wyprowadzenia złącza eSATA na zewnątrz obudowy.Płyta zawierająca min. następujące gniazda PCIe:- 1 x PCI Express 3.0 x16,- 1 x PCI Express 3.0 x16 (x4 elektrycznie),- 2 x PCI Express 3.0 x1Płyta główna komputera musi wpierać obsługę systemu kodowania korekcyjnego ECC dla pamięci RAM oraz procesora zaoferowanego komputera. |
|  | Procesor | Procesor klasy x86, osiągający wynik co najmniej 12000 pkt w teście SysMark w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie <http://www.cpubenchmark.net> w okresie od dnia ukazania się ogłoszenia oraz nie później niż jeden dzień przed składaniem oferty. |
|  | Pamięć operacyjna | 32GB GB UDIMM, 2400MHz DDR4, 4 sloty na pamięć. |
|  | Konfiguracja dyskowa | 1 dysk - 512GB SSD zawierający partycję RECOVERY umożliwiającą odtworzenie po awarii systemu operacyjnego, fabrycznie zainstalowanego na komputerze.2 dysk - min. 1TB SATA III |
|  | Napęd optyczny | Napęd DVD +/-RW (dopuszcza się zastosowanie napędu typu slim), wyposażony w zaczepy umożliwiające pracę w pionie i poziomie. |
|  | Karta graficzna | Dedykowana karta graficzna z własną pamięcią min. 4GB oraz min. 1024 rdzeniami CUDA wyposażona w cyfrowe wyjścia wideo min. 4 x DisplayPort |
|  | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  |
|  | Karta sieciowa | 10/100/1000 – złącze RJ45 WoL |
|  | Porty/złącza | - 8 x USB w tym: 1x USB3.0 z przodu obudowy i 6 z tyłu obudowy (z czego min. 3 x USB 3.0); - port sieciowy RJ-45, - port szeregowy RS-232- porty słuchawek i mikrofonu lub port combo na przednim lub tylnym panelu obudowy (z tyłu Line-out)Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
|  | Klawiatura/mysz | Klawiatura przewodowa w układzie US lub EU, USB, kabel min 1,5mMysz przewodowa 3 przyciskowa (scroll), USB, kabel min. 1,5m |
|  | Zasilacz | Zasilacz o mocy maksymalnej min. 400W o sprawności min. 90%, wraz z kablem zasilającym - złącza: Hybrydowe typu C/E/F męskie - IEC C13 ,min. 1.8m, kolor czarny |
|  | System operacyjny | Zainstalowany/preinstalowany nowy, nieaktywowany nigdy wcześniej na innym urządzeniu, system operacyjny: Oryginalny Windows 10 Pro. PL 64-bit z licencją lub równoważny.Parametry równoważności:* pełna integracja z systemami IBM Lotus Notes, SWOP, Płatnik;
* pełna obsługa ActiveX;
* dostępne dwa rodzaje graficznego interfejsu użytkownika, w tym: - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

- dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych;* możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
* wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
* wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
* system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);
* zgodny z posiadanym przez zamawiającego oprogramowaniem MS Office 2007/2010/2013/2016, oprogramowaniem IBM Tivoli Endpoint Manager for Lifecycle Management (wraz z instalacją agenta IBM TEM);
* oprogramowanie powinno umożliwiać zainstalowanie oprogramowania

(Kies, Active Sync lub Centrum obsługi urządzeń z systemem WindowsMobile, PC Suitę lub Nokia Suitę, Zune, iTunes) umożliwiającego pełną synchronizację i zgrywanie kontaktów i danych między używanymi przez Zamawiającego telefonami komórkowymi (Nokia, Iphone, Samsung, Telefunken) oraz komputerem.* oprogramowanie powinno zawierać certyfikat autentyczności lub unikalny kod aktywacyjny;

Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji Microsoft Windows 10 |
|  | BIOS  | BIOS zgodny ze specyfikacją UEFI Możliwość odczytania z Bios informacji o:- modelu komputera, - MAC Adres karty sieciowej,- zainstalowanym procesorze, jego taktowaniu - ilości pamięci RAM wraz z taktowaniem,- napędach lub dyskach podłączonych do portów SATA1-SATA6Możliwość z poziomu Bios:- wyłączenia selektywnego (pojedynczego) portów SATA- zdefiniowania tygodniowej agendy automatycznego włączania komputera- ustawienia hasła: administratora, Power-On, HDD, - zmiany trybu pracy kontrolera SATA pomiędzy AHCI, RAID- wyłączenia karty sieciowej, karty audio, portu szeregowego, - alertowania zmiany konfiguracji sprzętowej komputera - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - załadowania optymalnych ustawień Bios- obsługa Bios za pomocą klawiatury - obsługa Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
|  | Zintegrowany System Diagnostyczny | Narzędzie działające bez udziału systemu operacyjnego czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera. Oprogramowanie musi umożliwiać:- wykonanie testu pamięci RAM - wykonanie testu dysku twardego |
|  | Certyfikaty i standardy | Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-9001 (lub równoważny). Dokument należy załączyć do oferty.Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-14001 (lub równoważny). Dokument należy załączyć do oferty.Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-50001 (lub równoważny). Dokument należy załączyć do oferty.Deklaracja zgodności CE. Dokument należy załączyć do oferty.Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. |
|  | Waga/rozmiary urządzenia | Suma wymiarów nie może przekroczyć: 1060mmWaga maks. 13 kg. |
|  | Bezpieczeństwo i zdalne zarządzanie | * Złącze typu Kensington Lock
* Dedykowane oczko na kłódkę umożliwiające zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy
* Moduł TPM 2.0
* Zamek w obudowie nie wystający poza obrys
 |
|  | Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site)W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego.W przypadku potrzeby przekazania sprzętu do serwisu poza miejscem użytkowania, zostanie on wysłany bez dysku twardego.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Oświadczenie producenta należy dołączyć do oferty. |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.- możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

|  |  |
| --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne monitora |
| Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą TFT 27”  |
| Rozmiar plamki (maksymalnie) | 0,311 mm |
| Jasność | 250 cd/m2 |
| Kontrast | 1000:1, dynamiczny 4 000 000:1 |
| Kąty widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy(maksymalnie) | 6 ms (gray to gray) |
| Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
| Częstotliwość odświeżania poziomego |  30 – 82 kHz |
| Częstotliwość odświeżania pionowego |  56 – 76 Hz |
| Pochylenie monitora | W zakresie 26 stopni |
| Wydłużenie w pionie | Tak, min 130 mm |
| PIVOT | Tak |
| Powłoka powierzchni ekranu | Antyodblaskowa |
| Podświetlenie | System podświetlenia LED |
| Zużycie energii | Typowo 18W, maksymalne 38W, czuwanie mniej niż 0,33W |
| Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Lock |
| Waga bez podstawy | Maksymalnie 4,60kg |
| Waga z podstawą | Maksymalnie 7,50kg |
| Złącze  | 1x 15-stykowe złącze D-Sub, 1x HDMI (v1.4), 1x złącze DisplayPort (v1.2)2 x USB 3.0 1 USB 3.0 port - upstream |
| Gwarancja | 3 lata na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczegoFirma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.Gwarancja zero martwych pikseli |
| Certyfikaty | ISO 13406-2 lub ISO 9241,  |
| Inne | Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnejOdłączany stand VESA 100mmGłośniki zintegrowane w obudowie lub dedykowane z możliwością podłączenia do obudowy lub zewnętrzne w kolorze czarnym- w zestawie kabel zasilający złącza: Hybrydowe typu C/E/F męskie - IEC C13 ,min. 1.8m, kolor czarny oraz - kabel HDMI - HDMI 1.8m- kabel DisplayPort – DisplayPort min. 1.8m- kabel USB 3.0 min. 1.8m |

Zadanie nr 3 - Dostawy terminali monitoringu CCTV

**Wzór-Załącznik nr 1c do SIWZ**

**Zadanie nr 3**

**OFERTA WYKONAWCY**

Pełna nazwa Wykonawcy: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*

Adres: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*

Nr telefonu i faksu, adres e-mail:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*

Osoba/osoby uprawnione do reprezentacji, w tym do podpisania umowy ramowej: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\*

**Przystępując do postępowania prowadzonego w celu zawarcia umowy ramowej w trybie przetargu nieograniczonego na „Dostawy zestawów komputerowych”, WZP-4651/18/204/Ł – zadanie nr 1 – Dostawy terminali monitoringu CCTV**

**I. Oferujemy:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.p. | Nazwa przedmiotu zamówienia | j.m. | Cena jednostkowa netto w PLN | Stawka podatku VAT | Cena jednostkowa brutto w PLN(kol. 4 + 4 x 5) |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | **Terminal monitoringu CCTV – typ A** Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | kpl. | …..........................\*\* | ……%\* | …...............................\*\* |
| 2 | **Terminal monitoringu CCTV – typ B** Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | zest. | …..........................\*\* | ……%\* | …...............................\*\* |
| 3 | **Terminal monitoringu CCTV – typ C** Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | zest. | …..........................\* | ……%\* | …..........................\* |
| 4 | **Terminal monitoringu CCTV – typ D**Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | zest. | …..........................\* | ……%\* | …..........................\* |
| 5 | **Terminal monitoringu CCTV – typ E** Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | kpl. | …..........................\* | ……%\* | …..........................\* |
| 6 | **Terminal monitoringu CCTV – typ F** Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie …………………………………..\* | kpl. | …..........................\* | ……%\* | …..........................\* |
| 7 | **Terminal monitoringu CCTV – typ G**Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | zest. | …..........................\* | ……%\* | …..........................\* |
| 8 | **Terminal monitoringu CCTV – typ H**Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera)System operacyjny ………………………………\*Oprogramowanie zabezpieczające ………………………………………………………...\* | zest. | …..........................\* | ……%\* | …..........................\* |
| 9 | **Sprzętowy serwer plików wideo**Producent ……………………………………………\*(pełna nazwa lub oznaczenie modelu definiująca konfigurację sprzętową komputera) | Szt. | …..........................\* | ……%\* | …..........................\* |

* 1. **Oferujemy wykonywanie dostaw asortymentu w terminie do …………… (max. 21 – min. 3) dni roboczych,** licząc od dnia zawarcia umowy wykonawczej.
	2. **Oświadczamy, że:**
1. Podpisany dokument elektroniczny formularza JEDZ został zaszyfrowany tj. opatrzony hasłem dostępowym w brzmieniu ...............................................................................................\*
2. Oferowany asortyment wraz z oprogramowaniem jest zgodny z wymaganiami Zamawiającego wskazanymi w załączniku nr 2c do SIWZ.
3. ..............\*\*\* (**min. 24) miesięcznej gwarancji**;
4. ..............\*\*\* (**min. 24) miesięcznej rękojmi** za wady dostarczonego asortymentu

– liczonych od dnia podpisania przez Strony bez uwag protokołu odbioru końcowego dostawy.

1. Jest możliwość telefonicznego lub przez stronę internetową ……………………\* sprawdzenia konfiguracji sprzętowej terminali po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
2. Dostęp do najnowszych sterowników i uaktualnień jest na stronie internetowej producenta lub jego przedstawiciela.
3. Jesteśmy/nie jesteśmy\*\*\*\* małym przedsiębiorstwem /średnim przedsiębiorstwem\*\*\*\*.
4. Jesteśmy/nie jesteśmy\*\*\*\*\* podmiotem uprawnionym do udzielania licencji i dostawy oprogramowania, o którym mowa w Rozdz. II pkt 6 SIWZ;
5. Zgodnie z ustawą o podatku od towarów i usług obowiązek odprowadzenia podatku VAT leży po stronie Wykonawcy/Zamawiającego \*\*\*\*\*\*.
6. Zawarte w Rozdz. XVII SIWZ ogólne warunki umowy zostały przez nas zaakceptowane i w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy ramowej na warunkach tam określonych w miejscu i terminie wskazanym przez Zamawiającego.
7. Uważamy się za związanych niniejsza ofertą na czas wskazany w SIWZ tj. **60 dni** od upływu terminu składania ofert.
8. Warunki płatności: **30 dni,** licząc od daty otrzymania przez Zamawiającego faktury.
9. Zobowiązujemy się do zapewnienia możliwości odbierania wszelkiej korespondencji związanej z prowadzonym postępowaniem przez całą dobę na numer faksu .....................................................\*, lub e-mail:.....................................................................................\*.
10. Będziemy niezwłocznie potwierdzać fakt otrzymania wszelkiej korespondencji od Zamawiającego na nr faksu lub e-mail wskazany w Rozdz. I pkt 7 SIWZ.
11. W przypadku braku potwierdzenia faktu otrzymania korespondencji, Zamawiający ma prawo uznać, że korespondencja została skutecznie przekazana.
12. Pod groźbą odpowiedzialności karnej, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień otwarcia ofert..

**III. Informujemy, że:**

1. Dostawy wykonywane będą własnymi siłami/z pomocą Podwykonawcy\*\*\*\*\*\*\* .......................................................................................\* *(nazwa firmy, siedziba)*,któremu powierzona będzie część zamówienia obejmująca …................................................................\*
2. Zaproszenie do złożenia oferty w postępowaniu w ramach umowy ramowej będzie wysyłane na nr faksu …………..\* lub adres e-mail *……………………………………..\**
3. Reklamacje, zlecenia i zamówienia należy składać w dni robocze (od poniedziałku do soboty) w godzinach 8:00÷16:00na adres: ....................................................................................\*, nr faksu .................................................\*, e-mail ...................................................................\*
4. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu2).

1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (tj. Dz. Urz. UE L 119 z 04.05.2016 r., str. 1).

2) W przypadku, gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

 **PODPIS I PIECZĘĆ WYKONAWCY**

 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Uwaga:

*\* - należy wpisać*

*\*\* - należy wpisać, z dokładnością do dwóch miejsc po przecinku*

*\*\*\* - należy wpisać, jeżeli Wykonawca nie wpisze, Zamawiający uzna, że Wykonawca zaoferował okres gwarancji/rękojmi wskazany w nawiasie*

*\*\*\*\* - niepotrzebne skreślić*

\**\*\*\*\* - niepotrzebne skreślić, jeżeli Wykonawca nie dokona skreślenia, Zamawiający uzna, że Wykonawca nie jest podmiotem uprawnionym do udzielania licencji i dostawy oprogramowania*

\**\*\*\*\*\* - niepotrzebne skreślić, jeżeli Wykonawca nie dokona skreślenia, Zamawiający uzna, że obowiązek odprowadzenia podatku VAT z tytułu dostawy leży po stronie Wykonawcy*

*\*\*\*\**\**\*\* - niepotrzebne skreślić, w przypadku nieokreślenia lub nie uzupełnienia informacji o Podwykonawcy, Zamawiający uzna, iż Wykonawca będzie realizował zamówienie własnymi siłami .*

OPIS PRZEDMIOTU ZAMÓWIENIA

**Dostawa Terminali monitoringu CCTV**

***1.Terminal monitoringu CCTV* w obudowie RACK 19” *– Typ A – 4 komplety***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z wyposażeniem dodatkowym |
| 2. | Zastosowania | Terminal będzie wykorzystywany dla potrzeb aplikacji IP HD Video CCTV Genetec Security, aplikacji biurowych, aplikacji obliczeniowych, dostępu do intranetu oraz firmowej poczty elektronicznej. |
| 3. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |

|  |  |
| --- | --- |
| Cechy urządzenia | Wymagania Minimalne |
|  |  | System Operacyjny | Windows 10 Professional 64-bit PL lub inny równoważny, umożliwiający instalację oprogramowania będącego w dyspozycji Zamawiającego - Genetec Security. Zgodny z wymaganiami dla oprogramowania (Software Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji.  |
|  |  | **Oprogramowanie zabezpieczające** | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |
|  |  | **Procesor** | Ósmej generacji procesor Intel Core zgodny z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
|  |  | **Karta Graficzna** | 2 x NVIDIA® Quadro® P400 2GB lub równoważna umożliwiająca jednoczesne wyświetlenie obrazu na czterech monitorach, zgodna z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
|  |  | **Pamięć Operacyjna** | 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
|  |  | Pamięć Masowa | 512 GB SSD PCIe M.2 Opal; 1 TB 2.5" Serial-ATA (7,200 RPM) Hard Drive |
|  |  | **Napęd Optyczny** | DVD ROM, SATA |
|  |  | **Karta Sieciowa** | 1x1Gbit Network Card |
|  |  | **Obudowa** | Max 2U, przystosowana do montażu w szafie RACK, szyny i elementy montażowe w zestawie |
|  |  | **Klawiatura** | USP (QWERTY)  |
|  |  | **Mysz** | USB Optyczna |
|  |  | Kabel Zasilający | 220V; dł. min. 1,5m |
|  |  | Szyny montażowe do szafy Rack | TAK – dedykowane do zastosowanej obudowy |
|  |  | Zasilacz | Single, Hot-plug Power Supply 550 W, 80Plus Platinium |
|  |  | **Wsparcie Techniczne** | Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony |
|  |  | **Warunki Gwarancji** | 2-letnia gwarancja producenta świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego, |

1. ***Terminal monitoringu w obudowie tower – Typ B – 5 zestawów***

|  |  |  |  |
| --- | --- | --- | --- |
| **I** | **Cechy urządzenia** |  | Ilość |
| 1. | Typ | Terminal z monitorem i wyposażeniem dodatkowym |  |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |  |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |  |
| 5. | Procesor | Minimum jeden procesor 8 generacji Intel Core i7, min. 3,5 GHz i 8MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Genetec.  |  |
| 6. | Płyta główna | Płyta główna wyposażona w: * min. 2 złącza PCI Express x16 (Gen. 3)
* min. 1 złącze PCI Express x8
* min. 4 złączy SATA w tym min. 2 sztuki SATA 3.0
* kontroler dysków z obsługą funkcji RAID 0/1/
* min. 2 złącza DDR4 z obsługą do 64GB pamięci RAM
 |  |
| 7. | Gniazda we/wy | * min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0. Dwa z nich, w tym jeden port 3.0 muszą być umieszczone z przodu obudowy, pozostałe w tym jeden port 3.0 na tylnym panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.;
* port słuchawek i mikrofonu,
 |  |
| 8. | Pamięć operacyjna | 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |  |
| 9. | Pamięć masowa | * HDD 1 x 0,5TB SATA 7200 RPM (dane)
* SSD 256GB (system operacyjny)
 |  |
| 10. | Napęd optyczny | * Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”)
 |  |
| 11. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P2000 lub równoważna o parametrach:* PCIex16 z min. 5 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
* maksymalna rozdzielczość w trybie cyfrowym 5120 x 2880
* umożliwiająca niezależne wyświetlenie 4 pulpitów
 |  |
| 12. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |  |
| 13 | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |  |
| 14 | Obudowa | * Obudowa, umożliwiająca pracę w pionie jak i w poziomie.
* Obudowa musi umożliwiać serwisowanie stacji bez użycia narzędzi.
* Moduł konstrukcji obudowy w jednostce centralnej stacji powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów).
* Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady antykradzieżowej) lub kłódki (oczko w obudowie do założenia kłódki).
* Wbudowany czujnik otwarcia obudowy nie może zajmować dostępnych na płycie slotów PCI,
 |  |
| 15 | Zasilacz | * Zasilacz min. 630W pracujący w sieci 230V 50/60Hz prądu zmiennego.
 |  |
| 16. | System operacyjny | * System operacyjny np.: Windows 10 Professional x64 PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacyjnym IP HD Video CCTV, Genetec – współpracujący z posiadanym przez zamawiającego systemem, zapewniający pełną funkcjonalność oprogramowania Genetec Security Desk w wersji 5.5 lub nowszej oraz wymienionych do niego akcesoriów .
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |  |
| 17 | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |  |
| 18. | Klawiatura | * Klawiatura USB (czarna) układ klawiszy QWERTY
 |  |
| 19. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |  |
| 20. | Kabel zasilający | * Długość min 1,5 metra
 |  |
| 21. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |  |
| 22. | Wsparcie techniczne producenta | * Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony.
 |  |
| 23. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem  |  |
| 24. | Przewód HDMI (M) – HDMI (M) | - dł. min 3 metry |  |
| 25. | Przewód DVI (M) – DVI (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem |  |
| 26. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem  |  |
| 27. | Przewód HDMI (M) – HDMI (M) | - dł. Min 10 metrów |  |
| 28. | Przewód DVI (M) – DVI (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem |  |
| 29. | Patchcord RJ45 – RJ45 | - przewód RJ45 UTP kat. min 6 - przewód umożliwiający połączenie karty sieciowej komputera z gniazdem  ściennym sieci komputerowej.- dł. min 4 metry |  |

1. ***Terminal monitoringu w obudowie tower – Typ C – 20 zestawów***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z monitorem i wyposażeniem dodatkowym |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
| 4. | Procesor | Minimum jeden procesor 8 generacji Intel Core i7, min. 3,2 GHz i 12MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Genetec.  |
| 5. | Płyta główna | Płyta główna wyposażona w: * min. 2 złącza PCI Express x16 (Gen. 3)
* min. 1 złącze PCI Express x8
* min. 4 złączy SATA w tym min. 2 sztuki SATA 3.0
* kontroler dysków z obsługą funkcji RAID 0/1/
* min. 2 złącza DDR4 z obsługą do 64GB pamięci RAM
 |
| 6. | Gniazda we/wy | * min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0. Dwa z nich, w tym jeden port 3.0 muszą być umieszczone z przodu obudowy, pozostałe w tym jeden port 3.0 na tylnym panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.;
* port słuchawek i mikrofonu,
 |
| 7. | Pamięć operacyjna | 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
| 9. | Pamięć masowa | * HDD 1 x 0,5TB SATA 7200 RPM (dane)
* SSD 256GB PCIe (system operacyjny)
 |
| 9. | Napęd optyczny | * Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”)
 |
| 10. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P620 lub równoważna o parametrach:* PCIex16 z min. 2 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
* maksymalna rozdzielczość w trybie cyfrowym 5120 x 2880
* umożliwiająca niezależne wyświetlenie 4 pulpitów
 |
| 11. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |
| 12. | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |
| 13. | Obudowa | * Obudowa, umożliwiająca pracę w pionie jak i w poziomie.
* Obudowa musi umożliwiać serwisowanie stacji bez użycia narzędzi.
* Moduł konstrukcji obudowy w jednostce centralnej stacji powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów).
* Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady antykradzieżowej) lub kłódki (oczko w obudowie do założenia kłódki).
* Wbudowany czujnik otwarcia obudowy nie może zajmować dostępnych na płycie slotów PCI,
 |
| 14. | Zasilacz | * Zasilacz min. 630W pracujący w sieci 230V 50/60Hz prądu zmiennego.
 |
| 15. | System operacyjny | * System operacyjny np.: Windows 10 Professional x64 PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacyjnym IP HD Video CCTV, Genetec – współpracujący z posiadanym przez zamawiającego systemem, zapewniający pełną funkcjonalność oprogramowania Genetec Security Desk w wersji 5.5 lub nowszej oraz wymienionych do niego akcesoriów .
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |
| 16. | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |
| 17. | Klawiatura | * Klawiatura USB (czarna) układ klawiszy QWERTY
 |
| 18. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |
| 18. | Kabel zasilający | * Długość min 1,5 metra
 |
| 20. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |
| 21. | Wsparcie techniczne producenta | * Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony.
 |
| 22. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem  |
| 23. | Przewód HDMI (M) – HDMI (M) | - dł. min 3 metry |
| 24. | Przewód DVI (M) – DVI (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem |
| 25. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem  |
| 26. | Przewód HDMI (M) – HDMI (M) | - dł. Min 10 metrów |
| 27. | Przewód DVI (M) – DVI (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem |
| 28. | Patchcord RJ45 – RJ45 | - przewód RJ45 UTP kat. min 6 - przewód umożliwiający połączenie karty sieciowej komputera z gniazdem  ściennym sieci komputerowej.- dł. min 4 metry |
| 29. | Zewnętrzny Dysk USB | - typ: magnetyczny;- Format szerokości: 2.5 cala;- interfejs: USB 3.0;- Pojemność: 2 TB;- max transfer: 600 MB/s |
| 30. | Monitor mały terminala | Wymagane minimalne parametry |  |
|  | Typ ekranu | LED / LCD |  |
|  | Przekątna ekranu | od 25” do 27” |  |
|  | Jasność | nie mniej niż 250 cd/m2 |  |
|  | Kontrast | nie mniej niż 1000:1 |  |
|  | Kąty widzenia (pion/poziom) | nie mniej niż 160/160 stopni |  |
|  | Czas reakcji matrycy | max 6ms |  |
|  | Rozdzielczość  | nie mniej niż 3840 x 2160  |  |
|  | Format ekranu | 16:9 |  |
|  | Regulacja wysokości ekranu | TAK |  |
|  | Powłoka powierzchni ekranu | Antyodblaskowa  |  |
|  | Złącze  | Natywne wejścia min. 1xDVI-D, 1xHDMI, 1xDisplayPort |  |
|  | Certyfikaty | * Energy Star 5.0,
* Certyfikat może być dostarczony w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |  |
|  | Inne | * Monitor muszą posiadać uniwersalny system mocowania w standardzie VESA.
 |  |

1. ***Terminal monitoringu w obudowie tower – Typ D – 10 zestawów***

|  |  |  |  |
| --- | --- | --- | --- |
| **I** | **Cechy urządzenia** |  | Ilość |
| 1. | Typ | Terminal z monitorem i wyposażeniem dodatkowym |  |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Avigilon Control Center ACC dla ostatniej i najnowszej wersji.<http://avigilon.com/support-and-downloads/for-software/acc/system-requirements/>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |  |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |  |
| 4. | Procesor | Minimum jeden procesor 8 generacji Intel Core i5, min. 3,5 GHz i 8MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Avigilon.  |  |
| 5. | Płyta główna | Płyta główna wyposażona w: * min. 1 złącze PCI Express x16 (Gen. 3)
* min. 1 złącze PCI Express x8
* min. 2 złączy SATA w tym min. 2 sztuki SATA 3.0
* kontroler dysków z obsługą funkcji RAID 0/1/
* min. 2 złącza DDR4 z obsługą do 64GB pamięci RAM
 |  |
| 6. | Gniazda we/wy | * min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0. Dwa z nich, w tym jeden port 3.0 muszą być umieszczone z przodu obudowy, pozostałe w tym jeden port 3.0 na tylnym panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.;
* port słuchawek i mikrofonu,
 |  |
| 7. | Pamięć operacyjna | 8GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Avigilon Control Center dla ostatniej i najnowszej wersji. |  |
| 8. | Pamięć masowa | * HDD 1 TB SATA 7200 RPM
 |  |
| 9. | Napęd optyczny | * Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”)
 |  |
| 10. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P620 lub równoważna o parametrach:* PCIex16 z min. 2 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
* maksymalna rozdzielczość w trybie cyfrowym 5120 x 2880
* umożliwiająca niezależne wyświetlenie 4 pulpitów
 |  |
| 11. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |  |
| 12. | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |  |
| 13. | Obudowa | * Obudowa, umożliwiająca pracę w pionie jak i w poziomie.
* Obudowa musi umożliwiać serwisowanie stacji bez użycia narzędzi.
* Moduł konstrukcji obudowy w jednostce centralnej stacji powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów).
* Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady antykradzieżowej) lub kłódki (oczko w obudowie do założenia kłódki).
* Wbudowany czujnik otwarcia obudowy nie może zajmować dostępnych na płycie slotów PCI,
 |  |
| 14. | Zasilacz | * Zasilacz min. 300W pracujący w sieci 230V 50/60Hz prądu zmiennego.
 |  |
| 15. | Klawiatura | * Klawiatura USB (czarna) układ klawiszy QWERTY
 |  |
| 16. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |  |
| 17. | Kabel zasilający | * Długość min 1,5 metra
 |  |
| 18. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |  |
| 19. | Wsparcie techniczne producenta | * Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony.
 |  |
| 20. | Oprogramowanie Windows Pro 10 MOLP PL GOV | - typ licencji: rządowa;- rodzaj licencji: nowa licencja;- okres licencji: wieczysta; |  |
| 16. | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |  |
| 21 | Monitor mały terminala | Wymagane minimalne parametry | 1 szt. |
|  | Typ ekranu | LED / LCD |  |
|  | Przekątna ekranu | od 24” do 27” |  |
|  | Jasność | nie mniej niż 250 cd/m2 |  |
|  | Kontrast | nie mniej niż 1000:1 |  |
|  | Kąty widzenia (pion/poziom) | nie mniej niż 160/160 stopni |  |
|  | Czas reakcji matrycy | max 6ms |  |
|  | Rozdzielczość  | nie mniej niż 1920 x 1080  |  |
|  | Format ekranu | 16:9 |  |
|  | Regulacja wysokości ekranu | TAK |  |
|  | Powłoka powierzchni ekranu | Antyodblaskowa  |  |
|  | Złącze  | Natywne wejścia min. 1xDVI-D, 1xHDMI, 1xDisplayPort |  |
|  | Certyfikaty | * Energy Star 5.0,
* Certyfikat może być dostarczony w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |  |
|  | Inne | * Monitor muszą posiadać uniwersalny system mocowania w standardzie VESA.
 |  |

1. ***Terminal systemu monitoringu w obudowie mobilnej – Typ E – 8 kpl.***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z wbudowanym wyświetlaczem LED 15,6 cali |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
| 5. | Procesor | Minimum jeden procesor 8 generacji Intel Core i7, min. 2,6 GHz i 8MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Genetec.  |
| 7. | Gniazda we/wy | * min. 3 portów USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0.
* port słuchawek i mikrofonu,
* 1 x HDMI;
 |
| 8. | Pamięć operacyjna | * 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji.
 |
| 9. | Pamięć masowa | * HDD 1 TB SATA 5400 RPM (dane)
* SSD 256GB PCIe (system operacyjny)
 |
| 10. | Napęd optyczny | * Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”)
 |
| 11. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P2000 lub równoważna o parametrach:* PCIex16 z min. 4 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
 |
| 12. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |
| 13 | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |
| 16. | System operacyjny | * System operacyjny np.: Windows 10 Professional x64 PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacyjnym IP HD Video CCTV, Genetec – współpracujący z posiadanym przez zamawiającego systemem, zapewniający pełną funkcjonalność oprogramowania Genetec Security Desk w wersji 5.5 lub nowszej oraz wymienionych do niego akcesoriów .
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |
|  | Bateria | * Litowo-jonowoa w zestawie
 |
| 18. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |
| 19. | Kabel zasilający | * Długość min 1,5 metra
 |
| 20. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |
| 21. | Wsparcie techniczne producenta | * Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony.
 |

1. ***Terminal systemu monitoringu w obudowie mobilnej – Typ F –5 kpl.***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z wbudowanym wyświetlaczem LED 15,6 cali |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
| 4. | Procesor | Minimum jeden procesor 8 generacji Intel Core i7, min. 2,2 GHz i 8MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Genetec.  |
| 5. | Gniazda we/wy | * min. 3 porty USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0.
* port słuchawek i mikrofonu,
* 1 x Thunderbold;
* 1 x HDMI
 |
| 6. | Pamięć operacyjna | 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
| 7. | Pamięć masowa | * HDD 1 TB SATA 5400 RPM (dane)
* SSD 256GB PCIe (system operacyjny)
 |
| 8. | Napęd optyczny | Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”) |
| 9. | Karta graficzna | Karta grafiki np.: NVIDIA GeForce GTX 1060 lub równoważna o parametrach:* PCIex16 z min. 4 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
 |
| 10. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |
| 11. | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |
| 12. | System operacyjny | * System operacyjny np.: Windows 10 Professional x64 PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacyjnym IP HD Video CCTV, Genetec – współpracujący z posiadanym przez zamawiającego systemem, zapewniający pełną funkcjonalność oprogramowania Genetec Security Desk w wersji 5.5 lub nowszej oraz wymienionych do niego akcesoriów .
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |
| 13. | Bateria | * Litowo-jonowoa w zestawie
 |
| 14. | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |
| 15. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |
| 16. | Kabel zasilający | * Długość min 1,5 metra
 |
| 17. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |
| 18. | Wsparcie techniczne producenta | Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony. |
| 19. | Zewnętrzny Dysk USB | - typ: magnetyczny;- Format szerokości: 2.5 cala;- interfejs: USB 3.0;- Pojemność: 2 TB;- max transfer: 600 MB/s | 3 szt. |
| 20. | Dysk twardy HDD | - pojemność 6 TB- interfejs: SATA 6 Gb/s- format obudowy: 3,5”- Klasa obr/min: 5400;- Pamięć podręczna 64MB | 3 szt. |

1. ***Terminal systemu monitoringu w obudowie tower – Typ G – 2 zestawy***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z monitorem i wyposażeniem dodatkowym |
| 2. | Zgodność z systemami operacyjnymi i standardami | Oferowane elementy terminali muszą być zgodne z wymaganiami w zakresie Client Station Requirements oraz Software Requirements umieszonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. <http://www.genetec.com/search-results?q=System+Requirements>Terminal musi pozwalać na jednoczesne wyświetlenie obrazu z min. 16 kamer Full HD (1920x1080) |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
| 4. | Procesor | Minimum jeden procesor Intel Core 8 generacji, min. 3,2 GHz i 12MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji IP HD video CCTV, Genetec.  |
| 5. | Płyta główna | Płyta główna wyposażona w: * min. 2 złącza PCI Express x16 (Gen. 3)
* min. 1 złącze PCI Express x8
* min. 4 złączy SATA w tym min. 2 sztuki SATA 3.0
* kontroler dysków z obsługą funkcji RAID 0/1/
* min. 2 złącza DDR4 z obsługą do 64GB pamięci RAM
 |
| 6. | Gniazda we/wy | * min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 2 porty USB 3.0. Dwa z nich, w tym jeden port 3.0 muszą być umieszczone z przodu obudowy, pozostałe w tym jeden port 3.0 na tylnym panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.;
* port słuchawek i mikrofonu,
 |
| 7. | Pamięć operacyjna | 16GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej (Client Station Requirements) umieszczonymi na oficjalnej stronie producenta platformy Genetec Security dla ostatniej i najnowszej wersji. |
| 8. | Pamięć masowa | * HDD 1 x 0,5TB SATA 7200 RPM (dane)
* SSD 256GB PCIe (system operacyjny)
 |
| 9. | Napęd optyczny | * Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”)
 |
| 10. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P620 lub równoważna o parametrach:* PCIex16 z min. 2 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
* maksymalna rozdzielczość w trybie cyfrowym 5120 x 2880
* umożliwiająca niezależne wyświetlenie 4 pulpitów
 |
| 11. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |
| 12 | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |
| 13 | Obudowa | * Obudowa, umożliwiająca pracę w pionie jak i w poziomie.
* Obudowa musi umożliwiać serwisowanie stacji bez użycia narzędzi.
* Moduł konstrukcji obudowy w jednostce centralnej stacji powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów).
* Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady antykradzieżowej) lub kłódki (oczko w obudowie do założenia kłódki).
* Wbudowany czujnik otwarcia obudowy nie może zajmować dostępnych na płycie slotów PCI,
 |
| 14 | Zasilacz | * Zasilacz min. 630W pracujący w sieci 230V 50/60Hz prądu zmiennego.
 |
| 15. | System operacyjny | * System operacyjny np.: Windows 10 Professional x64 PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacyjnym IP HD Video CCTV, Genetec – współpracujący z posiadanym przez zamawiającego systemem, zapewniający pełną funkcjonalność oprogramowania Genetec Security Desk w wersji 5.5 lub nowszej oraz wymienionych do niego akcesoriów .
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |
| 16. | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |
| 17. | Klawiatura | * Klawiatura USB (czarna) układ klawiszy QWERTY
 |
| 18. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |
| 19. | Kabel zasilający | * Długość min 1,5 metra
 |
| 20. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |
| 21. | Wsparcie techniczne producenta | * Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony.
 |
| 22. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem  |
| 23. | Przewód HDMI (M) – HDMI (M) | - dł. min 3 metry |
| 24. | Przewód DVI (M) – DVI (M) | - dł. min 3 metry - umożliwiający połączenie karty graficznej z monitorem |
| 25. | Przewód DisplayPort (M) – DisplayPort (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem  |
| 26. | Przewód HDMI (M) – HDMI (M) | - dł. Min 10 metrów |
| 27. | Przewód DVI (M) – DVI (M) | - dł. min 10 metrów - umożliwiający połączenie karty graficznej z monitorem |
| 28. | Patchcord RJ45 – RJ45 | - przewód RJ45 UTP kat. min 6 - przewód umożliwiający połączenie karty sieciowej komputera z gniazdem  ściennym sieci komputerowej.- dł. min 4 metry |
| 29. | Zewnętrzny Dysk USB | - typ: magnetyczny;- Format szerokości: 2.5 cala;- interfejs: USB 3.0;- Pojemność: 2 TB;- max transfer: 600 MB/s |
| **30.** | **Monitor terminala** | **Wymagane minimalne parametry** |  |
|  | Typ ekranu | LED/LCD |  |
|  | Przekątna ekranu | od 45” do 49” |  |
|  | Łączność bezprzewodowa | Bluetooth 4.0, WiFi |  |
|  | Głośniki | System 2.1 (40W) |  |
|  | Rozdzielczość  | nie mniej niż 3840 x 2160  |  |
|  | Format ekranu | 16:9 |  |
|  | Złącze  | Natywne wejścia min. 4xHDMI, 3xUSB, 1 x Ethernet |  |
|  | Inne | * Monitor muszą posiadać uniwersalny system mocowania w standardzie VESA.
* Smart TV
 |  |
| **31.** | **Uchwyt do monitora** | **Wymagane minimalne parametry** |  |
|  | Typ uchwytu | uchylny |  |
|  | Przekątna ekranu | od 45” do 49” |  |
|  | Max. obciązenie | 25 kg |  |
|  | Standard VESA | 100x100, 200x100, 200x200, 300x200, 300x300, 400x200, 400x400 |  |
|  | Regulacja w pionie | 13 stopni |  |
|  | Regulacja w pionie  | 180 stopni |  |
|  | Max. Odległość od ściany | 422 mm |  |
|  | Min. Odległość od ściany | 62 mm |  |

1. ***Terminal monitoringu w obudowie tower – Typ H – 10 zestawów***

|  |  |  |
| --- | --- | --- |
| **I** | **Cechy urządzenia** |  |
| 1. | Typ | Terminal z monitorem i wyposażeniem dodatkowym |
| 2. | Zgodność z systemami operacyjnymi i standardami | Terminal będzie wykorzystywany dla potrzeb aplikacji Systemu Kontroli Dostępu I/Net Seven, aplikacji obliczeniowych, aplikacji biurowych |
| 3. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
| 4. | Procesor | Minimum jeden procesor 8 generacji Intel Core i5, min. 3,0 GHz i 9MB cache lub równoważny, w celu zapewnienia zgodności z istniejącym i planowanym środowiskiem aplikacji SKD I/Net Seven.  |
| 5. | Płyta główna | Płyta główna wyposażona w: * min. 1 złącza PCI Express x16 (Gen. 3)
* min. 1 złącze PCI Express x8
* min. 4 złączy SATA w tym min. 2 sztuki SATA 3.0
* kontroler dysków z obsługą funkcji RAID 0/1/
* min. 2 złącza DDR4 z obsługą do 64GB pamięci RAM
 |
| 6. | Gniazda we/wy | * min. 2 porty USB wyprowadzonych na zewnątrz komputera w tym min 1 port USB 3.0. Dwa z nich, w tym jeden port 3.0 muszą być umieszczone z przodu obudowy, pozostałe w tym jeden port 3.0 na tylnym panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.;
* port słuchawek i mikrofonu,
 |
| 7. | Pamięć operacyjna | 4GB lub więcej, zgodnie z rekomendowanymi wymaganiami dla stacji klienckiej I/Net Seven |
| 9. | Pamięć masowa | * HDD 1 x 0,5TB SATA 7200 RPM (dane)
* SSD 256GB PCIe (system operacyjny)
 |
| 9. | Napęd optyczny | Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt ( zamawiający dopuszcza urządzenie typu „slim”) |
| 10. | Karta graficzna | Karta grafiki np.: NVIDIA Quadro P400 lub równoważna o parametrach:* PCIex16 z min. 2 GB pamięci własnej GDDR5, ze wsparciem dla Open GL 4.5. Microsoft Direct X 12
* maksymalna rozdzielczość w trybie cyfrowym 1920 z 1080
* umożliwiająca niezależne wyświetlenie 2 pulpitów
 |
| 11. | Karta dźwiękowa | * karta dźwiękowa zintegrowana z płytą główną.
 |
| 12. | Karta sieciowa | * karta sieciowa 10/100/1000 Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania
 |
| 13. | Obudowa | * Obudowa, umożliwiająca pracę w pionie jak i w poziomie.
* Obudowa musi umożliwiać serwisowanie stacji bez użycia narzędzi.
* Moduł konstrukcji obudowy w jednostce centralnej stacji powinien pozwalać na demontaż kart rozszerzeń i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów).
* Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady antykradzieżowej) lub kłódki (oczko w obudowie do założenia kłódki).
* Wbudowany czujnik otwarcia obudowy nie może zajmować dostępnych na płycie slotów PCI,
 |
| 14. | Zasilacz | * Zasilacz min. 300W pracujący w sieci 230V 50/60Hz prądu zmiennego.
 |
| 15. | System operacyjny | * System operacyjny np.: Windows 7 Professional 32-bit PL lub równoważny, zainstalowany i aktywowany. W celu zapewnienia zgodności z istniejącym i środowiskiem I/Net Seven.
* Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie oprogramowania.
 |
| 16. | Oprogramowanie zabezpieczające | * Produkt musi udostępniać mechanizm umożliwiający wprowadzenie polityki least privilege na systemach operacyjnych użytkowników końcowych i maszyn Windows
* W ramach jednej licencji proponowane rozwiązanie powinno realizować co najmniej funkcje: centralnego zarządzania podnoszeniem uprawnień obiektów systemu operacyjnego dla standardowych użytkowników (bez uprawnień administracyjnych), kontroli aplikacyjnej oraz blokowania kradzieży danych dostępowych z systemu operacyjnego oraz aplikacji
* Produkt musi posiadać funkcję wyświetlania okna użytkownikowi z opcjami wypełnienia formularza/uzasadnienia przed wykonaniem eskalacji uprawnień (musi istnieć możliwość definiowania, czy po wypełnieniu formularza użytkownikowi natychmiast podniosą się uprawnienia do poziomu administratora czy też musi czekać na akceptację działu bezpieczeństwa)
* Produkt musi umożliwiać automatyczne zbudowanie reguły w oparciu o zdarzenie wielokrotnie wykryte na różnych stacjach końcowych
* Produkt musi zapewniać wsparcie dla role-based access control (RBAC) poprzez definiowanie którzy administratorzy produktu mają mieć dostęp do poszczególnych komponentów interfejsu oraz trybu pracy (wyłącznie odczytu, modyfikacji)
* Produkt musi umożliwiać tworzenie reguł dla elementów takich jak: aplikacja, funkcje systemu operacyjnego, skrypty, activeX etc. Reguły uwzględniać muszą takie kryteria oraz mechanizmy jak: podnoszenie uprawnień obiektu, podnoszenie uprawnień obiektów z zaufanych źródeł, praca aplikacji na standardowych uprawnieniach, blokowanie obiektu, określenie uprawnień użytkownika do plików, katalogów, usług, pamięci zewnętrznych, zdefiniowanie ograniczeń oraz monitoringu ruchu aplikacji (do internetu, zasobów sieciowych, wykorzystania katalogów lokalnych oraz rejestrów, użycia pamięci innych procesów), definicja różnych reguł w różnych przedziałach czasu oraz sytuacjach w których użytkownik jest w sieci organizacji lub poza nią.
* Produkt musi umożliwiać monitoring nieznanych oraz niesklasyfikowanych aplikacji
* Produkt musi umożliwiać utrzymywanie listy dozwolonych aplikacji dla stacji niepodłączonych do domeny
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla Windows Catalog
* Przy definicji listy dozwolonych aplikacji produkt musi zapewniać wsparcie dla obiektów COM, DLL oraz skryptów
* Przy definicji listy dozwolonych aplikacji oraz podnoszeniu uprawnień produkt umożliwiać musi określenie zaufanych źródeł dla aplikacji, skryptów oraz innych chronionych obiektów, dzięki którym uruchomienie obiektu nie jest ograniczane przez utworzone wcześniej reguły. Wymagane jest wsparcie dla nie mniej niż następujących źródeł: zaufane systemy dystrybucji oprogramowania, producent, zasób sieciowy, updater, określony użytkownik wykonujący aktualizację, zdefiniowane paczki instalacyjne.
* Produkt musi umożliwiać implementację ograniczeń co najmniej takich jak zablokowanie dostępu do sieci publicznej oraz ograniczenie dostępu do zasobów sieci LAN dla danej aplikacji, grupy aplikacji oraz aplikacji niesklasyfikowanych, nieznanych (tworzenie szarej listy uruchamianych aplikacji)
* Produkt musi umożliwiać nagrywanie całej sesji użycia obiektu (np aplikacji) przez określonego użytkownika na określonej stacji. Musi istnieć możliwość zdefiniowania miejsca składowania nagrania oraz komunikatu wyświetlanego użytkownikowi o nagrywaniu przed uruchomieniem aplikacji.
* Rozwiązanie musi posiadać możliwość integracji z zewnętrznymi bazami reputacyjnymi (co najmniej Virustotal, NSRL) oraz rozwiązaniami Sandbox (wymagana integracja z rozwiązaniami FireEye, Checkpoint, Palo Alto) w celu sklasyfikowania nieznanych, podejrzanych aplikacji w celu wykrycia zagrożeń takich jak złośliwe oprogramowanie
* Rozwiązanie musi posiadać mechanizm raportowy pozwalający na wygenerowanie raportów:

-Wnioskowanie o podwyższenie uprawnień przez poszczególnych użytkowników -Inwentaryzacja przynależności użytkowników do grup uprzywilejowanych-Zablokowane działania aplikacji, próby uruchomienia aplikacji, uzasadnienia użycia wpisane przez użytkowników, nieautoryzowane odwołania aplikacji w środowisku sieciowym lub na dysku lokalnym- Pliki wykonywalne składowane na stacjach użytkowników- Wykorzystanie reguł polityki- Inwentaryzacja stacji oraz wykorzystywanych aplikacji agenckich- Integracji z systemami identyfikacji złośliwego oprogramowania (jakie zagrożenia zostały wykryte)- Aktywność administracyjna* Musi istnieć możliwość tworzenia własnego poziomu (niekoniecznie administrator / power user) na który mogą być podnoszone uprawnienia dla poszczególnych obiektów (np. aplikacji, funkcji systemu operacyjnego), czyli tzw. Custom tokens, w ramach których zdefiniowane muszą być nowe wymagania oraz przynależność do grup AD Security groups.
* Rozwiązanie musi chronić systemy operacyjne Windows XP, Vista, 7, 8/8.1, 10, Server 2003, 2008, 2012/R2, 2016
* Rozwiązanie musi posiadać funkcję wykrywania oraz blokowania wycieku danych dostępowych (haseł / skrótów) z mechanizmów SAM, LSASS, przeglądarek internetowych, aplikacji do sesji zdalnych, klientów bazodanowych, rejestrów, danych z kont serwisowych bez konieczności zakupu dodatkowych modułów / licencji. Musi istnieć możliwość określenia wykluczeń dla obiektów (aplikacji, skryptów) które mogą odwoływać się do opisanych w niniejszym punkcie repozytoriów poświadczeń.
* Narzędzie musi być dostarczone w postaci licencji nieograniczonej w czasie
 |
| 17. | Klawiatura | * Klawiatura USB (czarna) układ klawiszy QWERTY
 |
| 18. | Mysz | * Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) + podkładka
 |
| 19. | Kabel zasilający | * Długość min 1,5 metra
 |
| 20. | Certyfikaty i standardy | * Certyfikat ISO 9001:2000 lub ISO 9001 dla producenta sprzętu
* Terminal musi spełniać wymogi normy min. Energy Star 5.0.
* Certyfikaty mogą być dostarczone w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |
| 21. | Wsparcie techniczne producenta | Dostęp do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu terminala – do oferty należy dołączyć link strony. |
| 22. | Patchcord RJ45 – RJ45 | - przewód RJ45 UTP kat. min 6 - przewód umożliwiający połączenie karty sieciowej komputera z gniazdem  ściennym sieci komputerowej.- dł. min 4 metry |
| 23. | Zewnętrzny Dysk USB | - typ: magnetyczny;- Format szerokości: 2.5 cala;- interfejs: USB 3.0;- Pojemność: 2 TB;- max transfer: 600 MB/s |
| 24. | Monitor mały terminala | Wymagane minimalne parametry |  |
|  | Typ ekranu | LED / LCD |  |
|  | Przekątna ekranu | od 24” do 27” |  |
|  | Jasność | nie mniej niż 250 cd/m2 |  |
|  | Kontrast | nie mniej niż 1000:1 |  |
|  | Kąty widzenia (pion/poziom) | nie mniej niż 160/160 stopni |  |
|  | Czas reakcji matrycy | max 6ms |  |
|  | Rozdzielczość  | nie mniej niż 1920 x 1080  |  |
|  | Format ekranu | 16:9 |  |
|  | Regulacja wysokości ekranu | TAK |  |
|  | Powłoka powierzchni ekranu | Antyodblaskowa  |  |
|  | Złącze  | Natywne wejścia min. 1xDVI-D, 1xHDMI, 1xDisplayPort |  |
|  | Certyfikaty | * Energy Star 5.0,
* Certyfikat może być dostarczony w formie oświadczenia dostawcy o spełnieniu tego warunku.
 |  |
|  | Inne | * Monitor muszą posiadać uniwersalny system mocowania w standardzie VESA.
 |  |

1. ***Sprzętowy serwer plików wideo – typ I - 1 szt***

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| System operacyjny | Wbudowany Linux |
| Procesor CPU | Czterordzeniowy procesor AMD R-Series RX-421ND 2.1 GHz |
| Pamięć (RAM) | 8GB DDR4 |
| Flash | 512MB (DOM) |
| Liczba gniazd pamięci RAM | 4 (Max 64 GB; UDIMM DDR4) |
| Maks. liczba dysków HDD i SSD | 8 x 2,5” lub 3,5” SATA 6 Gb/s, 3 Gb/s |
| Kieszeń na dysk twardy wymieniany podczas pracy | TAK |
| Obsługa modułów rozszerzających | 1 (UX-1200U-RP, UX-800U-RP) |
| Gniazdo wewnętrznej pamięci | 2 x M.2 2280 SATA 6Gb/s slot |
| Porty gigabitowej sieci LAN | 4 |
| Ramka Jumbo (GbE) |   |
| 10GbE | 2 x SFP+ |
| Gniazdo rozszerzeń (PCIe) | 1 (preinstalowany moduł karty sieciowej SFP+ NIC) |
| USB 2.0 | 4 |
| USB 3.0 | 2 |
| USB 3.1 10Gbps | Optional via PCIe expansion |
| Wskaźniki LED | HDD 1–8, Status, LAN, USB, Zasilanie |
| Przyciski | Zasilanie, Reset |
| Format | 2U do montażu stelażowego |
| Temperatura | 0 - 40 °C |
| Specyfikacja zasilania | 250W, 100-240V AC, 50-60Hz, 3.5A |
| Pobór mocy: Tryb uśpienia HDD (W) | 35,52(z kartą sieciową 10GbE) |
| Pobór mocy: Tryb pracy, typowe (W) | 103,88 (z kartą sieciową 10GbE) |
| Natężenie dźwięku dB(A) | 35,9 |
| Sek. zapis, 64 KB (MB/s) | 1290 (10GbE x 2) |
| Sek. odczyt, 64 KB (MB/s) | 1567 (10GbE x 2) |
| Sek. zapis z 256-bitowym szyfrowaniem AES woluminu (MB/s) | 1315 (10GbE x 2) |
| Sek. odczyt z 256-bitowym szyfrowaniem AES woluminu (MB/s) | 1187 (10GbE x 2) |
| System plików: wewnętrzny dysk twardy | EXT4 |
| System plików: zewnętrzny dysk twardy | EXT3, EXT4, NTFS, FAT32, HFS+ |
|  |  |
| **Pozostałe parametry** | Port Trunking / agregacja łączy |
| Wykrywanie usługi sieciowej (UPnP i Bonjour) |
| Wirtualne sieci LAN (VLAN) |
| Wiązanie usług na podstawie interfejsów sieciowych |
| 256-bitowe szyfrowanie AES na podstawie wolumenów |
| 256-bitowe szyfrowanie AES folderów |
| Szyfrowanie dysków zewnętrznych |
| Mechanizm szyfrowania sprzętowego (niedostępny w niektórych krajach) |
| Przywracanie RAID |
| Powiększanie pojemności RAID online |
| RAID10+ hot spare |
| RAID10 |
| RAID 6+ hot spare |
| RAID 6 |
| RAID 5+ dysk zapasowy |
| RAID 5 |
| RAID 1 |
| RAID 0 |
| JBOD |
| Pojedynczy dysk |
| Globalny dysk Hot Spare |
| Kontroler domeny i serwer NTP |
| Obsługa ACL na poziomie folderów współdzielonych |
| Obsługa Windows ACL |
| Migawka |
| Replikacja zdalna w czasie rzeczywistym (Real-time Remote Replication, RTRR) |
| Uwierzytelnianie Microsoft Active Directory (AD) |
| Serwer i klient LDAP |
| Powiadomienia (e-mail, SMS) |
| Wake on LAN (WOL) |
| Zaplanowane włączanie i wyłączanie |
| SNMP (wersja 2 i 3) |
| Logowanie przez Telnet i SSH (tylko dla administratora) |
| Virtualization Station |
| Container Station |
| Qsirch (pamięć RAM serwera NAS >= 2 GB) |
| Serwer i klient Syslog |
| Serwer poczty |
| Serwer VPN (PPTP + OpenVPN + L2TP) |
| Obsługa VMware® |
| Obsługa Citrix |
| Port Trunking / agregacja łączy |
| Wykrywanie usługi sieciowej (UPnP i Bonjour) |
| Wirtualne sieci LAN (VLAN) |
| Wiązanie usług na podstawie interfejsów sieciowych |
| 256-bitowe szyfrowanie AES na podstawie wolumenów |
| 256-bitowe szyfrowanie AES folderów |
| Szyfrowanie dysków zewnętrznych |
| Mechanizm szyfrowania sprzętowego (niedostępny w niektórych krajach) |
| Przywracanie RAID |
| Powiększanie pojemności RAID online |
| RAID10+ hot spare |
| RAID10 |
| RAID 6+ hot spare |
| RAID 6 |
| RAID 5+ dysk zapasowy |
| RAID 5 |
| RAID 1 |
| RAID 0 |
| JBOD |
| Pojedynczy dysk |
| Globalny dysk Hot Spare |
| Kontroler domeny i serwer NTP |
| Obsługa ACL na poziomie folderów współdzielonych |
| Obsługa Windows ACL |