*Załącznik nr 2 do SWZ*

Opis Przedmiotu Zamówienia

Pakiet 1. Przełącznik sieciowy POE - UM szt. 1

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Switch POE 48 port + 4xSFP+** |
| **Porty RJ** | Minimum 48 porty 100/1000BastT umieszczonych z przodu obudowy ze wsparciem dla standardu 802.3at (PoE+) |
| **Porty SFP+** | Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy. |
| **Przepustowość** | Minimum 175 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) |
| **Wydajność** | Minimum 98 Mp/s |
| **Bufor pakietów** | Minimum 1 MB |
| **Pamięć RAM** | Minimum 4GB pamięci operacyjnej |
| **Pamięć  Flash** | Minimum 16GB (eMMC, CF, SSD, SD, eUSB, SPI Flash). |
| **Dedykowany port konsoli** | 1x USB-C |
| **Dedykowany port USB** | Minimum 1x USB 2.0 (niezależny od portu konsoli USB) |
| **Tablica adresów MAC** | Minimum 8000 pozycji |
| **Obsługa Jumbo Frames** | TAK |
| **Obsługa sFlow lub Netflow** | TAK |
| **Obsługa skryptów** | Minimum w języku Python |
| **Obsługa REST API** | TAK |
| **Obsługa RMON** | Minimum grupy 1,2,3 i 9 |
| **VLAN** | Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN |
| **Obsługa standardu 802.1v** | TAK |
| **Obsługa protokołu MVRP** | TAK |
| **Konsola** | Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne |
| **Spaning Tree** | Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) |
| **Obsługa Secure FTP/SCP** | TAK |
| **LACP** | Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) |
| **Obsługa SNTPv4 lub NTP** | TAK |
| **Wsparcie dla IPv6** | IPv6 host, dual stack, MLD snooping, ND snooping |
| **LLDP** | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) |
| **Mechanizmy związane z zapewnieniem jakości usług w sieci** | Prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting |
| **Obsługa uwierzytelniania użytkowników** | Zgodna z:   * 802.1x, * w oparciu o adres MAC i serwer RADIUS * w oparciu o stronę WWW * wielu użytkowników na tym samym porcie w tym samym czasie |
| **Obsługa autoryzacji logowania** | Za pomocą serwerów RADIUS albo TACACS+ |
| **Obsługa autoryzacji komend wydawanych do urządzenia** | Za pomocą serwerów RADIUS albo TACACS+ |
| **Wbudowany serwer DHCP** | TAK |
| **Obsługa funkcji (UDP) helper** | TAK |
| **Obsługa blokowania nieautoryzowanych serwerów DHCP** | TAK |
| **Obsługa mechanizmu DLDP** | Wykrywanie łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego |
| **Spanning Tree** | Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) |
| **Obsługa list kontroli dostępu (ACL)** | Bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP |
| **Warunki środowiskowe** | Zakres pracy od minimum 0 do 45°C |
| **Zasilanie POE** | Zasilacz zapewniający budżet mocy PoE na poziomie nie niższym niż 370W |
| **Parametry fizyczne** | Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 33 cm |
| **Licencje** | 1. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania 2. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |
| **Gwarancja/Wsparcie** | Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. |

1. Przełącznik sieciowy – UM/MOPS szt. 4

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Switch 48 port + 4xSFP+** |
| **Porty RJ** | Minimum 48 porty 100/1000BastT umieszczonych z przodu obudowy |
| **Porty SFP+** | Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy. |
| **Przepustowość** | Minimum 175 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) |
| **Wydajność** | Minimum 98 Mp/s |
| **Bufor pakietów** | Minimum 1 MB |
| **Pamięć RAM** | Minimum 4GB pamięci operacyjnej |
| **Pamięć  Flash** | Minimum 16GB (eMMC, CF, SSD, SD, eUSB, SPI Flash). |
| **Dedykowany port konsoli** | 1x USB-C |
| **Dedykowany port USB** | Minimum 1x USB 2.0 (niezależny od portu konsoli USB) |
| **Tablica adresów MAC** | Minimum 8000 pozycji |
| **Obsługa Jumbo Frames** | TAK |
| **Obsługa sFlow lub Netflow** | TAK |
| **Obsługa skryptów** | Minimum w języku Python |
| **Obsługa REST API** | TAK |
| **Obsługa RMON** | Minimum grupy 1,2,3 i 9 |
| **VLAN** | Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN |
| **Obsługa standardu 802.1v** | TAK |
| **Obsługa protokołu MVRP** | TAK |
| **Konsola** | Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne |
| **Spaning Tree** | Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) |
| **Obsługa Secure FTP/SCP** | TAK |
| **LACP** | Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) |
| **Obsługa SNTPv4 lub NTP** | TAK |
| **Wsparcie dla IPv6** | IPv6 host, dual stack, MLD snooping, ND snooping |
| **LLDP** | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) |
| **Mechanizmy związane z zapewnieniem jakości usług w sieci** | Prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting |
| **Obsługa uwierzytelniania użytkowników** | Zgodna z:   * 802.1x, * w oparciu o adres MAC i serwer RADIUS * w oparciu o stronę WWW * wielu użytkowników na tym samym porcie w tym samym czasie |
| **Obsługa autoryzacji logowania** | Za pomocą serwerów RADIUS albo TACACS+ |
| **Obsługa autoryzacji komend wydawanych do urządzenia** | Za pomocą serwerów RADIUS albo TACACS+ |
| **Wbudowany serwer DHCP** | TAK |
| **Obsługa funkcji (UDP) helper** | TAK |
| **Obsługa blokowania nieautoryzowanych serwerów DHCP** | TAK |
| **Obsługa mechanizmu DLDP** | Wykrywanie łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego |
| **Spanning Tree** | Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) |
| **Obsługa list kontroli dostępu (ACL)** | Bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP |
| **Warunki środowiskowe** | Zakres pracy od minimum 0 do 45°C |
| **Zasilacz** | Zintegrowany pobierający maksymalnie 40W |
| **Parametry fizyczne** | Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 33 cm |
| **Licencje** | 1. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania 2. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |
| **Gwarancja/Wsparcie** | Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. |

1. Access Point szt. 3

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Access Point WI-FI 6** |
| **WI-FI** | Musi obsługiwać standard WIFI6 (802.11ax). |
| **Anteny** | * Minimum wbudowane 4 anteny o charakterystyce dookólnej. * Minimum 4x4 MIMO dla 5 GHz * Minimum 2x2 MIMO dla 2,4 GHz. |
| **Moduły radiowe** | * 5 GHz powinien umożliwiać przesyłanie danych przynajmniej do 4,8 Gbps dla 4 strumieni przestrzennych * 2,4 GHz powinien umożliwiać przesyłanie danych przynajmniej do 570 Mbps dla 2 strumieni przestrzennych. |
| **Bluetooth** | Zintegrowana obsługa Bluetooth w wersji przynajmniej 5. |
| **Zigbee** | Obsługa standardu radia 802.15.4 (Zigbee) do wsparcia sensorów, tagów |
| **TPM** | Wbudowana platforma TPM (Trusted Platform Module) do zabezpieczenia kodu startu i danych wewnętrznych AP. |
| **Standardem WPA** | Zgodność ze standardem WPA, WPA2, WPA3 w wersji Personal i Enterprise. |
| **Porty RJ** | Minimum dwa interfejsy 1000Base-T z możliwością agregacji w standardzie LACP. Jeden z tych interfejsów powinien umożliwiać zestawić połączenia z prędkością 2500BASE-T |
| **Zasilanie** | Zasilanie przez PoE w standardzie 802.3at/bt. Maksymalny pobór mocy nie większy niż 22W. |
| **Warunki środowiskowe** | Zakres pracy od minimum 0 do 50°C |
| **Zarządzanie** | Powinien mieć możliwość zarządzania w standardzie SNMP oraz przez REST API |
| **Kontroler do zarządzania** | * Punkty dostępowe powinny posiadać sprzętowy lub wirtualny kontroler służący do grupowania AP w celu wspólnego zarządzania wszystkimi APekami z pojedynczego interfejsu graficznego. Kontroler ten powinien zarządzać domeną radiową wspólnie dla wszystkich wdrażanych AP. * Kontroler powinien być w wersji redundantnej, tzn. w przypadku pojedynczego punktu awarii powinna być możliwość przejęcia roli kontrolera przez inne urządzenie z tymi samymi funkcjonalnościami co pierwotny kontroler. |
| **Porty konsoli** | Punkt dostępowy powinien posiadać wbudowany port konsoli (USB lub RS232) do zarządzania i diagnostyki. |
| **Elementy montażowe** | Dedykowane uchwyty montażowe umożliwiające instalację urządzeń na suficie (kasetony) w komplecie z punktem dostepowym. |
| **Gwarancja/Wsparcie** | Punkt dostępowy powinien posiadać gwarancję producenta „lifetime limited warranty”, to znaczy przynajmniej przez okres 3 lat od jego wycofania ze sprzedaży przez producenta. Powinien również posiadać możliwość bezpłatnych aktualizacji wewnętrznego oprogramowania (firmware). |

1. Usługa wdrożenia i konfiguracji sieciowej szt. 1

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Usługa konfiguracji sieci LAN** |
| **Zakres Prac** | 1. Aktualizacja oprogramowania w instalowanych nowych przełącznikach (5 sztuk) do wersji uzgodnionych z Zamawiającym. 2. Aktualizacja oprogramowania w punktach dostępowych (3 sztuki) do wersji uzgodnionych z Zamawiającym. 3. Instalacja i konfiguracja przełącznika w MOPS:    1. Utworzenie VLAN id X.    2. Skonfigurowanie portów w trybie ACCESS VLAN X.    3. Skonfigurowanie adresu IP MGT w VLAN X.    4. Skonfigurowanie routingu (default-gateway).    5. Przełączenie urządzeń na nowy przełącznik i sprawdzenie komunikacji: Fortigate MOPS, serwer MOPS i stacji roboczych MOPS. 4. Instalacja i konfiguracja przełącznika „Serwerownia Parter”:    1. Utworzenie 6 VLANów: A, B, C, D, E, F.    2. Instalacja wkładki SFP+ 10G-LR w porcie UPLINK. Konfiguracja portu UPLINK w trybie TRUNK 802.1Q. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    3. Konfiguracja portów w trybie ACCESS VLAN A, B i C. Podział portów określi Zamawiający na etapie realizacji.    4. Konfiguracja adresu IP MGT w VLAN F i skonfigurowanie routingu (default-gateway).    5. Skonfigurowanie 2 portów 1GE w trybie TRUNK 802.1Q do podłączenia urządzeń Fortigate. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    6. Przełączenie do przełącznika stacji roboczych, w tym stacji roboczej SRP, routera SRP, podłączenie światłowodu do serwerowni na 2. Piętrze.    7. Sprawdzenie komunikacji między routerem i stacją roboczą SRP. 5. Rekonfiguracja klastra FG100F:    1. Konfiguracja jednego portu 1GE na każdym z urządzeń w trybie TRUNK.    2. Utworzenie na tych interfejsach VLANów A, B, D, E, F i przypisanie adresacji IP uzgodnionej z Zamawiającym.    3. Utworzenie osobnych reguł FW dla każdego z VLANu A, B, D, F zgodnie z wytycznymi podanymi przez Zamawiającego na etapie realizacji.    4. Podłączenie przełącznika „Serwerownia Parter” dwoma linkami i sprawdzenie działania na tym przełączniku komunikacji IP pomiędzy VLANami A, B, D, F w ramach ustawionych reguł FW. 6. Instalacja i konfiguracja przełącznika #1 „Serwerownia 2. Piętro”:    1. Utworzenie 6 VLANów: A, B, C, D, E, F.    2. Instalacja 2 wkładek SFP+ 10G-LR w portach UPLINK. Konfiguracja portów UPLINK w trybie TRUNK 802.1Q. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    3. Skonfigurowanie 3 grup portów LACP po 2 porty 1GE w trybie ACCESS lub TRUNK 802.1Q do podłączenia serwerów (Server0, Server1, Server2). Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    4. Skrosowanie światłowodu do przełącznika znajdującego się na parterze.    5. Podłączenie serwerów: Server0, Server1, Server2 do portów GbE w przełączniku.    6. Sprawdzenie komunikacji z przełącznikiem parter, Fortigate100F oraz serwerami. 7. Instalacja i konfiguracja przełącznika #2 z PoE „Serwerownia 2. Piętro”:    1. Utworzenie 6 VLANów: A, B, C, D, E, F.    2. Instalacja 2 wkładek SFP+ 10G-LR w portach UPLINK. Konfiguracja portów UPLINK w trybie TRUNK 802.1Q. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    3. Skonfigurowanie 3 portów 1GE w trybie TRUNK 802.1Q do podłączenia punktów dostępowych do sieci WLAN. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    4. Konfiguracja portów w trybie ACCESS VLAN A i B. Podział portów określi Zamawiający na etapie realizacji.    5. Podłączenie patchcordem światłowodowym do przełącznika #1, podłączenie trzech punktów dostępowych WLAN oraz przełączenie stacji roboczych. Sprawdzenie komunikacji stacji roboczych z Fortigate100F oraz z serwerami. 8. Instalacja i konfiguracja przełącznika #3 „Serwerownia 2. Piętro”:    1. Utworzenie 6 VLANów: A, B, C, D, E, F.    2. Instalacja wkładki SFP+ 10G-LR w porcie UPLINK. Konfiguracja portów UPLINK w trybie TRUNK 802.1Q. Konfiguracja ALLOWED VLAN zgodnie z wymogami Zamawiającego.    3. Konfiguracja portów w trybie ACCESS VLAN A i B. Podział portów określi Zamawiający na etapie realizacji.    4. Podłączenie kablem krosowym światłowodowym do przełącznika #2, przełączenie stacji roboczych. Sprawdzenie komunikacji stacji roboczych z Fortigate100F oraz z serwerami. 9. Instalacja i konfiguracja sieci WLAN:    1. Instalacja fizyczna punktów dostępowych w miejscach uzgodnionych z Zamawiającym.    2. Instalacja trzech kabli UTP Cat.6A (?) pomiędzy szafą „Serwerownia 2. Piętro” a punktami montażu AP. Przy AP zakończenie kabla wtykiem RJ45 Cat.6A. Od strony szafy krosowniczej instalacja panelu z gniazdkami RJ45 Cat.6A.    3. Konfiguracja trzech punktów dostępowych w jeden klaster, wspólną domenę radiową.    4. Konfiguracja połączenia klastra AP z kontrolerem domeny Windows jako serwerem służącym do uwierzytelniania.    5. Konfiguracja trzech sieci SSID. Dwie sieci WLAN1, WLAN2 powinny być uwierzytelniane w oparciu o preshared key, zaś jedna WLAN3 z wykorzystaniem username/password pobieranym z kontrolera domeny.    6. Konfiguracja 3 stacji roboczych i sprawdzenie poprawności działania sieci WLAN1, WLAN2 i WLAN3. 10. Szkolenie z obsługi wdrożonego rozwiązania: konfiguracja przełączników, prace administracyjne na przełącznikach, konfiguracja sieci WLAN, dodawanie nowych sieci WLAN i ich zabezpieczanie w oparciu o zewnętrzny serwer, proste czynności diagnostyczne w przypadku problemów podłączenia się do sieci WLAN. Wymiar ok. 6h. 11. Dokumentacja powykonawcza obejmująca opis konfiguracji przełączników, sieci WLAN oraz dodatkowe wpisy konfiguracyjne FG100F. |
| **Dostawa i montaż elementów sieciowych** | Zamawiający wymaga, aby Wykonawca zapewnił i dostarczył wszystkie niezbędne elementy do wykonania usług wskazanych powyżej, w tym m.in.:   1. Wkładki SFP+ do przełączników typ 10G-LR, 6 szt. 2. Kable krosowe światłowodowe SM 9/125 o długości minimum 3m, 4 szt. 3. Kable krosowe UTP Cat.6A. 4. Realizacja połączeń fizycznych. |

1. UPS 20 kVa wraz z instalacją szt. 1

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Dostawa i montaż zasilacza UPS 20 kVA on-line** |
| **Ogólny opis wymagań UPS** | Zasilacz UPS pracujący w topologii on-line VFI-SS-111, wg normy IEC 62040-3, o mocy 20kVA/20kW. UPS będzie wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny. Bypass wewnętrzny będzie posiadał zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040). UPS będzie zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo będzie wyposażony w zewnętrzny tor obejściowy (serwisowy, mechaniczny). Baterie akumulatorów, zapewniające czas podtrzymania 6 minut dla obciążenia 20kW, będą umieszczone wewnątrz zasilacza UPS. |
| **Dane techniczne UPS** | |
| **moc wyjściowa:** | 20 kVA/20 kW. |
| **ilość faz** | 3 fazy wejściowe i 3 fazy wyjściowe. |
| **sprawność** | W trybie on-line: minimum 95,6% w zakresie obciążenia 50-100% (do 99% w trybie oszczędzania energii). |
| **Tolerancja napięcia wejściowego prostownika** | Bez przejścia na pracę z baterii: 190/330 – 276/478 V przy obciążeniu 100%. |
| **częstotliwość wejściowa** | 50 Hz lub 60 Hz z tolerancją 40 Hz do 72 Hz |
| **cosφ wejściowy** | 0,99 przy 100% obciążenia |
| **cosφ wyjściowy** | 1 |
| **współczynnik szczytu** | 3:1 |
| **Wejściowe zniekształcenia THDi** | < 3% |
| **Wyjściowe THDu** | * dla obciążenia liniowego < 2% * dla obciążenia nieliniowego < 5% |
| **Panel komunikacyjny** | Urządzenie musi posiadać panel, w którym powinny być zainstalowane:   * gniazdo komunikacji RS-232 * gniazdo wyłącznika awaryjnego p.poż. |
| **Interfejsy komunikacyjne** | opcjonalnie: SNMP, Modbus RTU, styki przekaźnikowe |
| **Wyświetlacz LCD** | TAK, graficzny |
| **wyłącznik bateryjny** | osobny wyłącznik w każdym łańcuchu baterii wewnętrznych. |
| **Zabezpieczenie przed zwrotnym podaniem energii** | W sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040) w torze bypassu statycznego UPS. |
| **Ładowanie baterii** | Urządzenie wyposażone w system nieciągłego ładowania baterii. Należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta. |
| **Gwarancja/Wsparcie** | Minimum 24 miesiące |
| **Usługi instalacji** | |
| **Instalacja UPSa** | Dostawa i montaż urządzenia w pomieszczeniu Zamawiającego:   1. Odłączenie istniejącego urządzenia Legrand KEOR-T 3/3 30 kVA nr seryjny 1707P1083003, 2. Posadowienie nowego zasilacza UPS w miejscu zdemontowanego zasilacza Legrand KEOR-T 3. Podłączenie do istniejącej instalacji elektrycznej Zamawiającego, zgodnie z zaleceniami producenta oferowanego urządzenia. 4. Wykonanie niezbędnych modyfikacji w instalacji elektrycznej wymaganej do prawidłowego uruchomienia zasilacza UPS.   Uwaga: na wejściu UPS należy stosować zabezpieczenia 3-polowe (nie należy rozłączać przewodu neutralnego UPS). Do zabezpieczenia należy stosować wkładki bezpiecznikowe typu gG/gL. |
| **Uruchomienie UPSa** | Uruchomienie zasilacza przez autoryzowany serwis oferowanego urządzenia oraz przeprowadzenie szkolenia z obsługi zasilacza UPS w miejscu użytkowania dla obsługi technicznej (2 osoby).  Szkolenie musi obejmować niezbędne elementy jakie przewiduje dokumentacja DTR producenta. |

1. Oprogramowanie SIEM szt. 1

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Wdrożenie oprogramowania SIEM** |
| **Wymagania funkcjonalne dla systemu** | 1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL |
| 1. System musi pracować w oparciu o architekturę Linux. |
| 1. System musi mieć możliwość centralnego zbierania i zarządzania logami |
| 1. System działać w trybie zbliżonym do rzeczywistego |
| 1. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu. |
| 1. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu. |
| 1. System musi zapewniać efektywną obsługę co najmniej 5000 EPS lub 100 GB danych dziennie. |
| 1. System musi zapewniać retencję danych w okresie minimum 365 dni. |
| 1. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu. |
| 1. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska. |
| 1. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja. |
| 1. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu. |
| 1. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji |
| 1. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu. |
| 1. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2. |
| 1. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3. |
| 1. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer. |
| 1. Interfejs musi posiadać angielską lub polską wersję językową. |
| 1. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1). |
| 1. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem. |
| 1. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius. |
| 1. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej. |
| 1. System musi wspierać mechanizm logowania typu Single Sign On. |
| 1. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników. |
| 1. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami. |
| 1. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika. |
| 1. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień. |
| 1. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych. |
| 1. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie. |
| 1. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant. |
| 1. System musi pozwalać na tworzenie parserów z poziomu GUI. |
| 1. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning. |
| 1. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów. |
| 1. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP. |
| 1. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach. |
| 1. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych. |
| 1. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:    * Syslog,    * WEF,    * Flat file,    * Event log,    * WMI,    * SNMP trap,    * XML,    * JSON,    * JDBC/ODBC    * CSV,    * Email,   Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze stronffy Zamawiającego. |
| 1. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure. |
| 1. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem. |
| 1. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe. |
| 1. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów. |
| 1. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera. |
| 1. System musi posiadać predefiniowany zestaw parserów zdarzeń. |
| 1. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta. |
| 1. System musi wspierać geolokalizację zdarzeń na bazie adresów IP. |
| 1. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania. |
| 1. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. |
| 1. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach. |
| 1. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa. |
| 1. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. |
| 1. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu. |
| 1. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów. |
| 1. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym. |
| 1. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących. |
| 1. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:    * Wykrycia dowolnej treści w logach,    * Wykrycia wystąpienia wartości pola na wybranej liście,    * Wykrycia niewystępowania wartości pola na wybranej liście,    * Wykrycia zmiany jednego z kilku pól,    * Wykrycia zdarzeń występujących z zadaną częstotliwością,    * Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,    * Wykrycia zaniku Wiadomości,    * Wykrycia nowej wartości pola w zadanym okresie czasu,    * Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności. |
| 1. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów. |
| 1. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API. |
| 1. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. |
| 1. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych. |
| 1. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności. |
| 1. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu. |
| 1. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook. |
| 1. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów. |
| 1. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT. |
| 1. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących. |
| 1. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat). |
| 1. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu. |
| 1. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi. |
| 1. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule. |
| 1. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły. |
| 1. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie. |
| 1. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu. |
| 1. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami. |
| 1. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika. |
| 1. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny. |
| 1. Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online. |
| 1. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania. |
| 1. System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizy formatu Netflow w wersji min. V5, v9 oraz IPFIX z wykorzystaniem oficjalnych modułów dostarczanych przez producenta. |
| 1. System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, rentransmisji, Jitter, Server Response Time oraz Round Trip Time. |
| 1. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 2lat. |
| 1. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów. |
| 1. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych. |
| 1. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów. |
| 1. Support producenta musi być świadczony w formule minimum 8/5. |
| 1. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego. |
| 1. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie. |
| 1. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL. |
| 1. **System musi umożliwiać integrację z Mitre ATT@CK.** |
| **Lista źródeł** | 1. System musi zbierać i korelować logi z min. 50 urządzeń. |
| 1. Reguły korelacyjne, alerty i obsługa incydentów. |
| 1. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych. |
| 1. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1. |
| 1. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark. |
| 1. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST. |
| 1. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit’u i wykrywania ukrytych procesów, plików, portów. |
| 1. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows |
| 1. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP. |
| **Szkolenia** | 1. Szkolenie musi być prowadzone w języku polskim. |
| 1. Szkolenie odbędzie się w formie zdalnej. |
| 1. Wykonawca dostarczy voucher szkoleniowy dla 2 słuchaczy dla systemu SIEM. |
| 1. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim. |
| 1. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem. |
| **Wdrożenie** | 1. Opracowanie harmonogramu wdrożenia systemu SIEM. |
| 1. Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia. |
| 1. Przeprowadzenie instalacji i konfiguracji systemu SIEM. |
| 1. Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych. |
| 1. Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem. |
| 1. Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia. |
| 1. Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych. |
| 1. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego. |
| 1. Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji. |

1. Serwer MOPS wraz z wdrożeniem szt. 1

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Serwer RACK wraz z oprogramowaniem i uruchomieniem** |
| **Wymagania techniczne serwera MOPS** | |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * 10 slotów na dyski 2.5” * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 56 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. * Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | Zainstalowany Jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 266 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | 128GB DDR5 RDIMM 5600MT/s, |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | * Zainstalowane:   + 4x dysk SAS FIPS-140 o pojemności min. 2.4TB, Hot-Plug   + 4x dysk SSD SATA o pojemności min. 480GB, Hot-Plug * Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | Trzy sloty PCIe LP |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Wbudowane porty** | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W klasy Titanium. |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych. |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2022 Standard * 15x Windows Server 2022 User CAL |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 V3 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera * oraz z możliwością rozszerzenia funkcjonalności o: * Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej * Przesyłanie danych telemetrycznych w czasie rzeczywistym * Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze * Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring:   + ilość podłączonych oraz rozłączonych systemów   + stan podłączonych urządzeń   + informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów   + Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia   + informacje o statusie gwarancji dla poszczególnych urządzeń   + informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń   + informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.   + Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych   + Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.   + Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.   + Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.   + Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.   + Monitoring parametrów serwerów z informacją o minimum:     - Obciążeniu procesora     - Zużyciu pamięci RAM     - Temperaturze procesorów     - Temperaturze powietrza wlotowego     - Zużyciu prądu     - Zmianach w fizycznej konfiguracji serwera     - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.   + Monitoring parametrów pamięci masowych z informacją o minimum:     - Opóźnieniach     - IOPS     - Przepustowości     - Utylizacji kontrolerów     - Pojemność całkowita i dostępna     - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.     - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata     - Informacje o poziomie redukcji danych     - Informacje o statusie replikacji oraz snapshotów   + Monitoring parametrów przełączników sieciowych z informacją o minimum:     - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny     - Stanie komponentów: zasilacze, wentylatory     - Podłączonych hostach     - Ilości i statusu portów     - Utylizacji procesora     - Utylizacji poszczególnych portów     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania. * Raporty   + Możliwość generowania raportów dla serwerów zawierających informację o:     - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej     - Średnim obciążeniu: procesorów, pamięci RAM, IO,   + Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:     - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.   + Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.   + Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.   + Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia   + Urządzenie Producenta dostarczane w ramach postępowania   + Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego). * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android * Certyfikaty   + Oferowana platforma musi być zaprojektowana zgodnie ze standardami:     - ISO 27001     - NIST Security and Privacy Controls for Federal Information Systems and Organization     - CSA Cloud Control Matrix |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angielskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3a lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
| **Wykaz prac wdrożeniowych – Serwer dla MOPS** | |
| W ramach prac wdrożeniowych przeprowadzone zostaną następujące czynności. | |
| **Projekt realizacyjny:** | Analiza przedwdrożeniowa |
| Przedstawienie szczegółowej architektury wdrożenia |
| Dokumentacja projektowa |
| **Wdrożenie hosta Hyper-V** | Instalacja fizyczna oraz podłączenie hosta we wskazanej lokalizacji |
| Aktualizacja oprogramowania systemowego/układowego urządzenia, jeśli wymagane |
| Konfiguracja karty zarządzającej serwera |
| Konfiguracja sieciowa |
| Instalacja i konfiguracja systemu windows i roli Hyper-V na oferowanym serwerze |
| Przygotowanie template VM z windows na potrzeby migracji obecnego środowiska |
| Przygotowanie VM dla nowego kontrolera domeny |
| Wypromowanie i skonfigurowanie kontrolera domany - pierwszy DC dla nowej domeny |
| Konfiguracja polityk bezpieczeństwa dla domeny wg rekomendacji Microsoft i najlepszych praktyk (dns, gpo , security policy) |
| Wykonanie dokumentacji powdrożeniowej |

1. Serwer NAS szt. 4

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Serwer NAS w obudowie RACK** |
| **Obudowa** | Rack |
| **Procesor** | Minimum czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz) |
| **Pamięć RAM** | min. 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 32 GB |
| **Dyski** | Zainstalowane dyski twarde przeznaczone do pracy ciągłej. Oferowane dyski muszą znajdować się na liście kompatybilności producenta z oferowanym urządzeniem. Zainstalowane 4szt. o pojemności 8TB każdy. Gwarancja na dyski twarde musi pokrywać się z gwarancją oferowanego urządzenia. |
| **Możliwości rozbudowy** | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband |
| **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) |
| **Porty zewnętrzne** | Minimum:   * 2 porty USB 3.2.1 * 1 gniazdo rozszerzenia |
| **Porty sieciowe** | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * 1 port 10GbE RJ45 * Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8 |
| **Funkcja Wake on LAN/WAN** | Tak |
| **Gniazdo rozszerzeń PCIe 3.0** | Min. 1x 4-liniowe gniazdo x8 Gen. 3 |
| **Wentylator obudowy** | Min. 3 wentylatory 60 mm x 60 mm |
| **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| **Obsługiwane systemy plików** | Min.:   * Wewnętrzny: Btrfs, ext4 * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| **Zarządzanie pamięcią masową** | * Maksymalny rozmiar pojedynczego wolumenu: * 200 TB (wymagana pamięć 32 GB) * 108 TB * Minimalny liczba wewnętrznych wolumenów: 64 * Minimalny liczba obiektów iSCSI Target: 128 * Minimalny liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN |
| **Obsługiwane typy macierzy RAID** | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| **Funkcja udostępniania plików** | * Minimalna liczba kont użytkowników: 2 048 * Minimalna liczba grup użytkowników: 256 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000 |
| **Uprawnienia** | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| **Wirtualizacja** | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® |
| **Usługa katalogowa** | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. |
| **Bezpieczeństwo** | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| **Obsługiwane przeglądarki** | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach. |
| **Oprogramowanie** | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| **Konserwacja** | Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack. |
| **Zasilanie** | Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |
| **Gwarancja** | Wykonawca udzieli gwarancji:   * 3 lata na urządzenie główne * 1 rok na dodatkowe akcesoria montażowe (w postaci przesuwnych szyn rack). |

1. Usługa migracji i wdrożenia poczty szt. 1

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Dostawa i migracja środowiska poczty** |
| **Wymagany zakres wdrożenia:** | Przeprowadzenie analizy przedwdrożeniowej obejmującej założenia konfiguracji tenantu Microsoft |
| Przedstawienie koncepcji wdrożeniowej do akceptacji |
| Konfiguracja dzierżawy środowiska Microsoft 365:   * globalne skonfigurowanie tenantu Microsoft 365 na podstawie najlepszych praktyk (znakowanie firmowe, ustawienia ogólne, MFA, Passwordless, SSO), * Konfiguracja ADConnect, * Synchroniacja tożsamości z obecnym środowiskiem, * rozwiązywanie problemów konfiguracyjnych na tenancie Microsoft 365, * przydzielenie licencji do użytkowników zgodnie z zaleceniami, |
| Konfiguracja poczty:   * Wspólna przestrzeń nazw domen pocztowych (skonfigurowanie domeny pocztowej, stworzenie koegzystencji) * Konfiguracja przepływu poczty (zakres prac powinien obejmować wyłączenie z ruchu pocztowego starego serwera) * Testowe migracje skrzynek pocztowych dla grupy użytkowników oraz weryfikacja * Migracja produkcyjna * Stablizacja zmigrowanej poczty. * Rozwiązywanie powstałych problemów w obrębie poczty. * Szkolenie dla administratorów IT. |
| **Założenia:** | Migracja do 100 skrzynek pocztowych, |
| Skrzynki pocztowe powyżej 50 GB zamawiający zarchiwizuje we własnym zakresie, |
| Zamawiający udzieli dostępów koniecznych do realizacji prac, |
| Konfiguracja środowiska obejmuje konfiguracje środowiska Microsoft 365 dla poziomu funkcjonalności dla poziomu licencji business standard. |
| Migracja poczty będzie realizowana w paczkach po minimum 25 kont pocztowych (maksymalnie 4 paczki migracyjne), |
| Zamawiający zapewni dedykowaną maszynę na instalacje AADConnecta (min. Windows 2016), |
| **Licencja Microsoft:** | Dostawa licencji:   1. Exchange Online (plan 1) w ilości 90 sztuk, 2. Exchange Online (plan 2) w ilości 10 sztuk, |
| Okres ważności licencji 12 miesięcy |
| **Wymagania dotyczące Wykonawcy** | 1. Wykonawca prac wdrożeniowych zapewni zespół wdrożeniowy, który zadał odpowiednie egzaminy firmy Microsoft.   Zespół wdrożeniowy powinien zawierać osoby z poniższymi kompetencjami: |
| 1. Microsoft 365 Certified MS 101 / MS 102: Administrator Expert min. 4 osoby |
| 1. Threat Protection MS-500 Advanced specialization min. 4 osoby |
| 1. Microsoft Certified SC 400: Information Protection and Compliance Administrator Associate min. 1 osoba |
| 1. II. Kompetencje Microsoft: |
| 1. Wykonawca prac wdrożeniowych spełni minimum wymagań dotyczących posiadania odpowiednich kompetencji oraz doświadczenia branżowego w zakresie wdrażania rozwiązania Microsoft 365. Firma realizująca wdrożenie będzie partnerem technologicznym firmy Microsoft posiadająca odpowiedni status potwierdzający możliwość wykonywania wdrożeń rozwiązań Microsoft. Firma realizująca powinna posiadać w Microsoft status Solution Partnera w obszarze Modern Work. 2. Firma realizująca wdrożenie będzie posiadała odpowiednie specjalizacje technologiczne firmy Microsoft w zakresie wdrażanych elementów bezpieczeństwa. (Microsoft Specializations -Information Protection and Governance) |
| 1. Referencje |
| Wykonawca przedstawi minimum 2 różne referencje na realizację usług wdrożenia Microsoft 365 lub migracji z innych rozwiązań pocztowych do Exchange dla organizacji powyżej 100 użytkowników. Referencje powinny dotyczyć wdrożeń realizowanych nie dawniej niż 3 lat wstecz od momentu złożenia oferty. |
| 1. Gwarancja na wykonanie usług |
| Wykonawca udzieli gwarancji na wykonane prace wdrożeniowe przez okres 6 miesięcy od daty podpisania protokołu odbioru. |
| 1. Dedykowany opiekun projektu |
| Wykonawca zapewni dedykowaną osobę do koordynowania projektu pomiędzy zespołami Zamawiającego i Wykonawcy. |

1. Usługa przerowadzenia testów penetracyjnych szt. 1

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Testy penetracyjne** |
| **Przedmiot zamówienia** | Przedmiotem zamówienia jest wykonanie na rzecz Zamawiającego przez Wykonawcę usługi polegającej na przeprowadzaniu testów penetracyjnych infrastruktury IT z zastosowaniem metodologii Greenbox, w zakresie:   * przeprowadzania testów penetracyjnych infrastruktury IT, * sporządzania raportów z wykonanych usług. |
| **Cel zamówienia** | Celem zlecanych prac jest identyfikacja możliwie jak największej liczby podatności, które mogą stanowić zagrożenie dla bezpieczeństwa przetwarzanych i przechowywanych informacji oraz danych, a także usług biznesowych realizowanych przez systemy teleinformatyczne. Testy będą realizowane z zastosowaniem metodologii Greenbox, zapewniającej kompleksowe podejście do analizy zagrożeń w oparciu o realne scenariusze ataku. |
| **Zakres prac** | Sprawdzenie uruchomionych usług sieciowych. |
| Sprawdzenie kont systemowych. |
| Sprawdzenie mechanizmów uwierzytelniania i autoryzacji. |
| Sprawdzenie wdrożonych mechanizmów dostępu do zasobów. |
| Sprawdzenie uprawnień do zasobów. |
| Sprawdzenie wdrożonych mechanizmów instalacji aktualizacji. |
| Sprawdzenie wdrożonych mechanizmów tworzenia kopii zapasowych. |
| Sprawdzenie wdrożonych mechanizmów logowania zdarzeń. |
| Sprawdzenie wdrożonych mechanizmów administracji zdalnej. |
| Sprawdzenie wdrożonych mechanizmów zabezpieczenia systemu w fazie boot. |
| Sprawdzenie wdrożonych mechanizmów zarządzania systemem. |
| Sprawdzenie wdrożonych dodatkowych metod ochrony. |
| Wskazanie zaleceń hardening’owych dla systemu operacyjnego. |
| **Audyt bezpieczeństwa infrastruktury** | Audyt architektury bezpieczeństwa infrastruktury IT. |
| Audyt konfiguracji urządzeń sieciowych. |
| Testy penetracyjne zewnętrzne:   * Identyfikacje dostępnych serwisów sieciowych, określenie oraz weryfikacja ich podatności; * Penetracja systemu za pomocą skanerów TCP i UDP; * Bezpieczeństwo aplikacji oraz usług dostępnych z zewnątrz * Analiza topologii sieci widzianej z zewnątrz; * Możliwość uzyskania nieautoryzowanego dostępu do danych; * Badanie podatności związanych atakami typu DDoS; * Konfiguracja komunikacji z usługami (np. konfiguracja SSL/TSL, IPsec); * Weryfikacja procedur zarządzania siecią WAN. |
| Testy penetracyjne wewnętrzne:   * Bezpieczeństwo urządzeń sieciowych; * Bezpieczeństwo protokołów trasowania; * Analiza topologii sieci i logiki jej segmentacji; * Bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze); * Bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz * maszynie, Istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia * bezprzewodowego wpiętego do sieci); * Filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja * pomiędzy kluczowymi podsieciami); * Konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji); * Możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych); * Przegląd danych dostępnych na udziałach sieciowych – weryfikujemy, czy możliwe jest * uzyskanie nieautoryzowanego dostępu do danych na udziałach sieciowych takich jak hasła * do systemów, czy też kluczowych dla działania organizacji danych; * Podatność na ataki DDoS; * Weryfikacja zasad bezpieczeństwa na wybranych stacjach roboczych; * Weryfikacja dostępu do Internetu z LAN; * Weryfikacja procedur zarządzania siecią LAN. |
| **Testy bezpieczeństwa** | Testy bezpieczeństwa będą obejmować testy penetracyjne infrastruktury IT, z zastosowaniem podejścia Greenbox. Metodologia ta zakłada częściowy dostęp do informacji o systemach, które są testowane. Dzięki wykorzystaniu tej metodologii pentesterzy mogą skuteczniej planować ataki, oraz dokładnie ocenić i zidentyfikować luki w zabezpieczeniach. |
| **Realizacja zadań** | Realizacja przedmiotu zamówienia odbywać się będzie co do zasady zdalnie, niemniej jednak w uzasadnionych przypadkach Zamawiający zakłada realizację zleconych prac w siedzibie Zamawiającego. Wykonawca będzie zobowiązany do obecności w siedzibie Zamawiającego, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania zlecenia jednostkowego. |
| **Raportowanie wyników** | Wykonawca zobowiązany jest wskazać w raporcie z realizacji zlecenia wszystkie zidentyfikowane podatności, w tym również te powszechnie znane na dzień wykonania zlecenia, jeżeli występują w weryfikowanej infrastrukturze lub sieci lokalnej. Za powszechnie znane podatności uznaje się co najmniej te wymienione w słowniku CVE. Raport będzie zawierał: |
| szczegółowy opis każdej zidentyfikowanej podatności, obejmujący sposób działania, wpływ na inne elementy infrastruktury oraz potencjalne konsekwencje, |
| rekomendacje dotyczące naprawy zidentyfikowanych podatności, |
| wykaz użytych narzędzi i oprogramowania |
| zabezpieczenie raportu przed dostępem osób nieuprawnionych. |
| **Narzędzia testowe** | Wszystkie testy bezpieczeństwa będą przeprowadzane za pomocą narzędzi Wykonawcy. Narzędzia te będą zgodne ze standardami branżowymi, wspierając metodologię Greenbox i umożliwiając realizację realistycznych scenariuszy ataku. |
| **Wymagania jakościowe** | Zamawiający oczekuje od Wykonawcy szczególnej staranności w zakresie wykonania przekazanych zleceń, z zastosowaniem "dobrych praktyk" i standardów związanych z realizacją prac w zakresie testów penetracyjnych infrastruktury IT. W ramach każdorazowego zlecenia, Wykonawca przedstawi raport, który będzie obejmował: |
| * listę zidentyfikowanych podatności, |
| * opis potencjalnych konsekwencji występowania podatności, |
| * szczegółowe propozycje naprawy podatności, |
| * użyte narzędzia i oprogramowanie, |
| * raport zabezpieczony przed dostępem osób trzecich. |

1. Szkolenie oraz kampania Phishingowa szt. 1

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Szkolenie oraz kampania Phishingowa** |
| **Kampania Phishingowa** | |
| **Cel Kampanii** | Celem kampanii phishingowej jest zwiększenie świadomości pracowników na temat zagrożeń związanych z phishingiem oraz ocena skuteczności istniejących procedur bezpieczeństwa w organizacji. Kampania ma na celu edukację pracowników na temat identyfikacji podejrzanych wiadomości e-mail i linków, a także poprawę ich umiejętności w zakresie reagowania na potencjalne zagrożenia. |
| **Zakres Kampanii** | Kampania obejmie wszystkie działy organizacji. Przewiduje się wysłanie symulowanych wiadomości phishingowych do pracowników, które będą naśladować typowe techniki używane przez cyberprzestępców. W ramach kampanii planuje się: |
| Przygotowanie i wysłanie 3-5 różnych typów wiadomości phishingowych. |
| Przeprowadzenie analizy reakcji pracowników na te wiadomości. |
| Oferowanie szkoleń i zasobów edukacyjnych dotyczących bezpieczeństwa w sieci. |
| **Metodologia** | Kampania zostanie przeprowadzona w kilku etapach: |
| Planowanie: Opracowanie scenariuszy phishingowych, które będą zgodne z aktualnymi trendami i technikami stosowanymi przez cyberprzestępców. |
| Wykonanie: Wysyłka symulowanych wiadomości phishingowych do wybranej grupy pracowników. |
| Ewaluacja: Analiza wyników kampanii, w tym liczba kliknięć w linki, raporty o podejrzanych wiadomościach oraz feedback od pracowników. |
| Raportowanie: Przygotowanie raportu podsumowującego wyniki kampanii oraz rekomendacje dotyczące dalszych działań edukacyjnych i zabezpieczeń. |
| **Oczekiwane Rezultaty** | Zwiększenie świadomości pracowników na temat zagrożeń związanych z phishingiem. |
| Zidentyfikowanie pracowników, którzy mogą potrzebować dodatkowego szkolenia w zakresie bezpieczeństwa. |
| Opracowanie planu działań w celu wzmocnienia procedur bezpieczeństwa w organizacji. |
| **Termin Realizacji** | Kampania powinna być zrealizowana w okresie 2 lat od złożenia zamówienia przez Zamawiającego, z raportem końcowym dostarczonym w ciągu 2 tygodni po zakończeniu kampanii. |
| Szkolenie dla pracowników urzędu w zakresie cyberbezpieczeństwa | |
| **Szkolenie dla pracowników urzędu w zakresie cyberbezpieczeństwa**  **Szkolenie z zakresu cyberbezpieczeństwa ma na celu rozwinięcie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych. W trakcie szkolenia uczestnicy zdobędą wiedzę na temat bezpieczeństwa informacyjnego w urzędzie, prawidłowej reakcji na cyberataki, a także podstawowych zasad i dobrych praktyk wykorzystywania technologii informatycznych. Praktyczne umiejętności zdobyte podczas kursu pozwolą na skuteczne zabezpieczenie danych i sprzętu.** | |
| **Szkolenie powinno zawierać co najmniej** | Definicja Cyberbezpieczeństwa i zakres odpowiedzialności pracowników. |
| Omówienie zasad bezpieczeństwa w Urzędzie. |
| Opis poprawnych zachowań oraz praktyk związanych z cyberbezpieczeństwem w miejscu pracy. |
| Bezpieczne korzystanie z systemów informatycznych. |
| Metody ochrony poufnych danych oraz unikanie ryzykownych zachowań online. |
| Informacje na temat zagrożeń w sieci takie jak malware, w tym ransomware, spoofing, vishing, phishing i inne ataki socjotechniczne, wyłudzenia informacji czy ataki fizyczne – wraz z przykładami. |
| Metody nieautoryzowanego pozyskiwania danych przez przestępców |
| Omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami. |
| Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja. |
| Stosowanie silnych haseł, autoryzacja dwuetapowa, klucze sprzętowe. |
| Metody przeciwdziałania wyłudzeniom danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń w urzędzie, szkodliwymi programami mogącymi pozyskać dane osobowe. |
| **Informacje dotyczące przeprowadzenia szkolenia** | Szkolenie w formie stacjonarnej w siedzibie Zamawiającego. |
| Szkolenie odbędzie się w 2 grupach po 30 pracowników w każdej grupie. |
| Czas trwania minimum 6 godzin zegarowe dla każdej grupy. |
| Liczba pracowników urzędu objętych szkoleniem – 60 pracowników. |
| Okres wykonania szkoleń - 2 lata od daty Zamówienia. |
| Forma szkolenia dostosowana do poziomu wiedzy, z założeniem, iż uczestnicy szkolenia mogą nie posiadać specjalistycznej wiedzy technicznej. |
| **Wymagania w zakresie przeprowadzenia szkolenia** | Wykonawca zapewni, iż posiada kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności z zakresu Cyberbezpieczeństwa udokumentowane odpowiednimi certyfikatami minimum. Security+, CISSP. |
| Zamawiający wymaga przygotowania harmonogramu i programu szkolenia i dostarczyenia w terminie nie później niż 10 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. |
| Wykonawca przygotuje i dostarczy materiały szkoleniowe dla każdego uczestnika szkolenia w postaci elektronicznej, które Zamawiający będzie mógł wykorzystać nieodpłatnie i wydrukować dla każdego uczestnika. Materiały muszą zawierać szczegółowe informacje, które będą omawiane podczas szkolenia. |
| Wykonawca dostarczy uczestnikom szkolenia ww. materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia. |
| Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca. |
| Sposób prowadzenia szkolenia przez prowadzącego musi umożliwiać uczestnikom zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym. |
| Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne zaświadczenia/certyfikaty potwierdzające ukończenie szkolenia i jego zakres; oraz zaświadczenie/certyfikat uzyska jednostka Zamawiająca. |
| Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:   * lista obecności uczestników szkolenia; * lista odbioru zaświadczeń o ukończeniu szkolenia; * ankieta satysfakcji ze szkolenia; |
| Wykonawca nie jest zobowiązany do zapewnienia uczestnikom szkolenia wyżywienia. |
| Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia wykonawcy w razie wykonania szkolenia na miejscu w siedzibie Zamawiającego. |

1. Oprogramowanie do zarządzania zasobami i procesami IT szt. 1

*Producent (wpisać) …………………………………………………………………….*

*Model urządzenia (wpisać) ……………………………………………………………*

Oprogramowanie ITManager z modułem sieciowym oraz backupu lub równoważne rozwiązanie. Za równoważność rozumie się produkt o parametrach nie gorszych, pod względem ilościowym i jakościowym, a w szczególności:

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Typ** | **Oprogramowanie do zarządzania zasobami i procesami IT** |
| **Wymagania ogólne** | Oprogramowanie posiada polski oraz angielski interfejs językowy. |
| Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej. |
| Oprogramowanie umożliwia obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą. |
| Odczyt informacji dotyczących parametrów sprzętowych komputera odbywa się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników. |
| Agent systemu nie nasłuchuje na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika. |
| Oprogramowanie umożliwia wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit. |
| Oprogramowanie posiada procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej umożliwia integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe posiada mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych. |
| Oprogramowanie posiada dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator. |
| Oprogramowanie posiada moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control). |
| Oprogramowanie umożliwia nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu). |
| Oprogramowanie umożliwia nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu). |
| Oprogramowanie umożliwia blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról. |
| Oprogramowanie współpracuje z serwerem MSSQL Server 2008R2-2019 |
| Oprogramowanie, w zakresie wszystkich warstw, nie wymaga do prawidłowej pracy komponentów Java. |
| Oprogramowanie serwera aplikacji posiada funkcjonalność centralnego wysyłania wybranych powiadomień mailowych . |
| Oprogramowanie posiada moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty. |
| Oprogramowanie jest podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (\*.exe), plików bibliotek współdzielonych (\*.dll), plików sterowników (\*.sys) oraz pakietów instalacyjnych oprogramowania (\*.msi). |
| Oprogramowanie agentów posiada obsługę sesji terminalowych Windows. |
| Oprogramowanie zapewnia dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online). |
| Oprogramowanie posiada raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej. |
| Oprogramowanie posiada mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość). |
| Oprogramowanie posiada mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego. |
| Oprogramowanie zapewnia automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU. |
| Oprogramowanie musi zapewnia w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. |
| Oprogramowanie posiada kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych. |
| Oprogramowanie umożliwia współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej. |
| Oprogramowanie umożliwia automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej. |
| Oprogramowanie posiada raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami. |
| Oprogramowanie umożliwia tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu). |
| Oprogramowanie umożliwia prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych. |
| Oprogramowanie umożliwia dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów. |
| Oprogramowanie umożliwia graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty. |
| Oprogramowanie umożliwia zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika. |
|  |
|  | Oprogramowanie umożliwia wydruk kartoteki sprzętowej stanowiska komputerowego. |
|  | Oprogramowanie umożliwia samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu. |
|  | Oprogramowanie umożliwia zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej. |
| **Inwentaryzacja konfiguracji komputerów** | Oprogramowanie umożliwiaa projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417 |
|  | Oprogramowanie umożliwia okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp. |
|  | Oprogramowanie Agenta umożliwia audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej. |
|  | Oprogramowanie umożliwia analizę sprzętową:   1. Płyty głównej w zakresie model, producent, nr. seryjny. 2. CPU w zakresie nazwy, modelu, producenta, częstotliwości. 3. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci. 4. RAM w zakresie wielkości pamięci. 5. karty sieciowej w zakresie model, adres IP, adres MAC. 6. karty graficznej w zakresie model. |
|  | Oprogramowanie umożliwia odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID. |
|  | Oprogramowanie umożliwia odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej. |
|  | Oprogramowanie umożliwia odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta. |
|  | Oprogramowanie umożliwia przegląd historii zmian parametrów sprzętowych komputerowych. |
|  | Oprogramowanie umożliwia globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych. |
|  | Oprogramowanie zawiera raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora. |
|  | Oprogramowanie umożliwia odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji). |
|  | Oprogramowanie umożliwia globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB. |
|  | Oprogramowanie umożliwia integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag). |
|  | Oprogramowanie umożliwia okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera). |
|  | Oprogramowanie umożliwia automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania. |
|  | Oprogramowanie umożliwia globalny przegląd wszystkich programów zainstalowanych na komputerach. |
|  | Oprogramowanie umożliwia tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.). |
|  | Oprogramowanie umożliwia tworzenie wykazów z zainstalowanym, dowolnie wybranym programem. |
|  | Oprogramowanie umożliwia tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach. |
| **Inwentaryzacja oprogramowania** | Oprogramowanie umożliwia tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu. |
|  | Oprogramowanie posiada wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office. |
|  | Oprogramowanie umożliwia oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji. |
|  | Oprogramowanie umożliwia zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika. |
|  | programowanie posiada globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji. |
| **Monitoring sieci LAN** | Oprogramowanie umożliwia okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony. |
| Oprogramowanie umożliwia monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru. |
| Oprogramowanie umożliwia wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router. |
| Oprogramowanie umożliwia z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową. |
| Oprogramowanie umożliwia monitorowanie stanu dowolnej usługi sieciowej TCP. |
| Oprogramowanie umożliwia monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia. |
| Oprogramowanie umożliwia monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING. |
| Oprogramowanie umożliwia tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email. |
| **Gwarancja/**  **Wsparcie** | **24 - miesiące** |