**Opis przedmiotu zamówienia**

1. **Serwer – 2 sztuki**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5” * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| **Procesor** | * Jeden procesor 8-rdzeniowy, min. 2.8GHz, umożliwiający osiągnięcie wyniku min. 89.8 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej. |
| **Pamięć RAM** | * 2x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s. |
| **Karta graficzna** | * Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |
| **Wbudowane porty** | * min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, * 1 port VGA na tylnym panelu, * 1 port RS232 |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe) * Dodatkowa karta Dual Port (2x RJ-45, 10Gb/s, 10GBase-T, PCIe) |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 |
| **Dyski twarde** | * Zainstalowane   + 2x dysk SSD SATA o pojemności min. 480GB, 12Gb, 2,5“ Hot-Plug. * Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Zasilacze** | * Redundantne, o mocy maks. 700W klasy Titanium |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * 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). |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **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. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. * 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](http://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 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * 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 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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. |

1. **Zarządzalne urządzenia sieciowe z obsługą VLAN – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| Lp. | Minimalne wymagania Zamawiającego | |
|  | CECHY SPRZĘTOWE | |
|  | Typ przełącznika | Zarządzany |
|  | Porty | • 16 Slotów SFP+ 10GE  • 1 Port konsolowy RJ45  • 1 Port konsolowy Micro-USB |
|  | Ilość wentylatorów | 1 |
|  | Zasilanie | 100-240 V AC~50/60 Hz |
|  | Montaż | Możliwość montażu w szafie rack |
|  | Układ | 1U |
|  | Maks. zużycie energii | 32.74 W |
|  | Ilość generowanego ciepła | 111,71 BTU/h |
|  | Wymagania systemowe | Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ lub Windows 7/8/10/11, MAC® OS, NetWare®, UNIX® lub Linux. |
|  | Certyfikaty | CE, FCC, RoHS |
|  | Środowisko pracy | • Dopuszczalna temperatura pracy: 0℃~40℃ (32℉~104℉);  • Dopuszczalna temperatura przechowywania: -40℃~70℃ (-40℉~158℉);  • Dopuszczalna wilgotność powietrza: 10%~90%, bez kondensacji  • Dopuszczalna wilgotność przechowywania: 5%~90%, bez kondensacji |
|  | WYDAJNOŚĆ | |
|  | Wydajność przełączania | 320 Gb/s |
|  | Szybkość przekierowań pakietów | 238.08 Mpps |
|  | Tablica adresów MAC | 32 K |
|  | Bufor pakietów | 24 Mb |
|  | Ramki jumbo | 9 KB |
|  | FUNKCJE OPROGRAMOWANIA | |
|  | Funkcja Quality of Service | • 8 kolejek priorytetowania  • Obsługa priorytetowania 802.1p CoS/DSCP  • Tryb harmonogramu priorytetowania:  - SP (Strict Priority)  - WRR (Weighted Round Robin)  - SP+WRR  • Kontrola przepustowości  - Ograniczanie prędkości transferu w oparciu o port/przepływ danych  • Płynniejsze działanie  • Działania dla przepływów  - Mirror (do obsługiwanego interfejsu)  - Redirect (do obsługiwanego interfejsu)  - Limit prędkości  - QoS Remark |
|  | Cechy przełącznika L3 | • 16 interfejsów IPv4/IPv6  • Routing statyczny  - 48 tras statycznych  • Wpisy statyczne ARP  - 128 wpisów statycznych  • Proxy ARP  • Gratuitous ARP  • Serwer DHCP  • DHCP Relay  - DHCP Interface Relay  - DHCP VLAN Relay  • DHCP L2 Relay |
|  | Funkcje L2 i L2+ | • Agregacja łączy  - Statyczna agregacja łączy  - LACP 802.3ad  - Do 8 grup agregacji i do 8 portów na grupę  • Protokół drzewa rozpinającego (STP)  - STP 802.1d  - RSTP 802.1w  - MSTP 802.1s  - Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona Root  • Wykrywanie pętli zwrotnych  - Oparte na portach  - Oparte na VLAN  • Kontrola przepływu  - Kontrola przepływu 802.3x  - Zapobieganie blokowaniu HOL  • Mirroring  - Port Mirroring  - Mirroring procesora  - Przesył One-to-One  - Przesył Many-to-One  - Port wejścia/wyjścia / obydwa porty |
|  | L2 Multicast | • IGMP Snooping  - IGMP v1/v2/v3 Snooping  - Fast Leave  - IGMP Snooping Querier  - Uwierzytelnianie IGMP  • Uwierzytelnianie IGMP  • MVR  • MLD Snooping  - MLD v1/v2 Snooping  - Fast Leave  - MLD Snooping Querier  - Konfiguracja grupy statycznej  - Ograniczone przekazywanie IP Multicast  • Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil |
|  | Funkcje zaawansowane | • Obsługa kontrolerów sprzętowych Omada (OC200/OC300), kontrolera programowego, kontrolera opartego na chmurze  • Automatyczne wykrywanie urządzeń  • Konfiguracje grupowe  • Grupowe aktualizacje oprogramowania  • Inteligentne monitorowanie stanu sieci  • Ostrzeżenia o nietypowych zdarzeniach  • Ujednolicony proces konfiguracji  • Harmonogram restartu  • Bezobsługowa konfiguracja ZTP |
|  | Sieci VLAN | • Grupy VLAN  - Maks. 4K grup VLAN  • Tagowanie 802.1Q VLAN  • Adres MAC VLAN: 30 wpisów  • Protokół VLAN  • Prywatna sieć VLAN  • GVRP  • VLAN VPN (QinQ)  - QinQ oparty na portach  - Selective QinQ  • Głosowa sieć VLAN |
|  | Listy kontroli dostępu | • Time-based ACL  • MAC ACL  - Source MAC  - Destination MAC  - VLAN ID  - User Priority  - Ether Type  • IP ACL  -Source IP  - Destination IP  - Fragment  - IP Protocol  - TCP Flag  - TCP/UDP Port  - DSCP/IP TOS  - User Priority  • Combined ACL  • Packet Content ACL  • IPv6 ACL  • Policy  - Mirroring  - Redirect  - Rate Limit  - QoS Remark  • ACL apply to Port/VLAN |
|  | Bezpieczeństwo transmisji | • Wiązanie adresów IP, MAC i portów  - 512 wpisów  - DHCP Snooping  - Inspekcja ARP  - Ochrona źródłowego adresu IPv4: 100 wpisów  • Wiązanie adresów IPv6, MAC i portów  - 512 wpisów  - DHCPv6 Snooping  - Wykrywanie ND  - Ochrona źródłowego adresu IPv6: 100 wpisów  • Ochrona przed atakami DoS  • Ochrona portów poprzez ich statyczną/dynamiczną konfigurację  - Do 64 adresów MAC na port  • Storm Control Broadcast/Multicast/Unicast  - tryb kontroli (kb/s/wskaźnik)  • Uwierzytelnianie 802.1X  - Uwierzytelnianie w oparciu o port  - Uwierzytelnianie w oparciu o adres MAC  - Przydzielanie VLAN  - MAB  - Sieć VLAN dla gości  - Uwierzytelnianie i autoryzowanie poprzez Radius  • AAA (w tym TACACS+)  • Izolacja portów  • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2  • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2  • Kontrola dostępu w oparciu o IP/port/MAC |
|  | IPv6 | • IPv6 Dual IPv4/IPv6  • Multicast Listener Discovery (MLD) Snooping  • ACL IPv6  • Interfejs IPv6  • Statyczny routing IPv6  • Funkcja neighbor discovery (ND) wykorzystywana przez węzły IPv6  • Path maximum transmission unit (MTU) discovery  • ICMP v6  • TCP v6/UDP v6  • Zastosowania protokołu IPv6:  - Klient DHCPv6  - Ping6  - Tracert6  - Telnet (v6)  - SNMP IPv6  - SSH IPv6  - SSL IPv6  - Http/Https  - TFTP IPv6 |
|  | ZARZĄDZANIE | |
|  | Funkcje panelu zarządzania | • Interfejs graficzny GUI  • Interfejs linii poleceń CLI  • SNMP v1/v2c/v3  - Trap/Inform  - RMON (grupy 1, 2, 3, 9)  • Szablon SDM  • Klient DHCP/BOOTP  • 802.1ab LLDP/LLDP-MED  • Autoinstalacja DHCP  • Dual Image, Dual Configuration  • Monitorowanie zużycia procesora  • Diagnostyka kabli  • EEE  • Odzyskiwanie hasła  • SNTP  • Logi systemowe |
|  | Dodatkowa wkładka | • Prędkość transmisji: 10 Gbps  • Typ: SFP  • Złącze wyjściowe: RJ45 |

1. **UTM – 1 sztuka**

**Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 10 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS  z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem  128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman  grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal  - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

**Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

**Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

**Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL  oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL  pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest  realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

**Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
7. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku

**Testy wydajnościowe oraz funkcjonalne**

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 12 miesięcy

**Gwarancja oraz wsparcie**

System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
3. **Macierz dyskowa – 1 sztuka**

|  |  |
| --- | --- |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”,    o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5” |
| Przestrzeń dyskowa | Zainstalowane:  12x dysk SAS o pojemności min. 1.2TB, Hot-Plug |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych. |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.  Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).  Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów SAS 12Gb (4 porty na kontroler), |
| Kable/wkładki | 2x kabel 12Gb HD Mini-SAS -HD Mini-SAS min. 4m |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.  Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.  Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold. |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta. Na żądanie Zamawiającego, Wykonawca musi  przedstawić oświadczenie producenta oferowanego serwera,  potwierdzające pochodzenie urządzenia z oficjalnego kanału  dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest  produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |
| Warunki gwarancji | 3 lata gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  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 przez producenta do 7 lat.  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.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |

1. **Oprogramowanie serwera – 4 sztuki**

**Wymagane minimalne parametry**

Oprogramowanie Windows Server 2022 Standard (licencja na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2022 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
10. zarządzania użytkownikami,
11. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
12. możliwości przydzielania praw dostępu do zasobów sieciowych,
13. instalacji zdalnej oprogramowania z pakietów msi,
14. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
15. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
16. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
17. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
18. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
19. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
20. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
21. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
22. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
23. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
24. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
25. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
26. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
27. System operacyjny musi posiadać obsługa PowerShelI 5.1,
28. System operacyjny musi posiadać obsługa certyfikatów w Active Directory
29. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

1. **Oprogramowanie serwera – 35 sztuk**

1. Licencje dostępowe na użytkownika

* Wymagana licencja typu Cal User OEM do systemu Windows Server 2022 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

1. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2022 na użytkownika:

* Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu User Cal z wdrożoną rolą Active Directory

1. **Oprogramowanie serwera – 5 sztuk**

1. Licencje dostępowe na urządzenie

* Wymagana licencja typu Device CAL OEM do systemu Windows Server 2022 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

1. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2022 na urządzenie:

* Licencja dostępowa na urządzenie umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu Device CAL z wdrożoną rolą Active Directory.
* Oprogramowanie równoważne musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania, przez nieograniczoną liczbę użytkowników korzystających ze wskazanej liczy urządzeń, funkcjonalności serwerowych systemów operacyjnych (z wyłączeniem dostępu terminalowego).

1. **Oprogramowanie przeciwdziałające wyciekowi danych – 35 sztuk**

**Oprogramowanie przeciwdziałające wyciekowi danych**- licencja wieczysta z 24 miesięcznym wsparciem.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera

zarządzającego z klientem odbywa się przy pomocy agenta.

1. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
2. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na

stacjach roboczych.

1. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
2. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość

lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z

serwerem administracyjnym.

1. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
2. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania:

kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych.

Administrator musi posiadać możliwość określenia wykonywania czasu związanego z

wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

1. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
2. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji

definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.

1. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu

jak i ich usuwania oraz klonowania.

1. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
2. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
3. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
4. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną

Active Directory.

1. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
2. logowanie oraz wylogowanie użytkownika,
3. włączenie oraz wyłączenie stacji roboczej,
4. blokada oraz odblokowanie stacji roboczej,
5. przejście w stan bezczynności stacji roboczej.

1. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
2. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika

końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.

1. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
2. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych,

aplikacji oraz typów plików.

1. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
2. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
3. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości

email.

1. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
2. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
3. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku

lub na wskazany adres(y) e-mail.

1. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta

oprogramowania.

1. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
2. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
3. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
4. aplikacje, z której zostały utworzone,
5. lokalizację,
6. adres URL,
7. format pliku,
8. zawartość pliku.
9. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno

lokalnych jak i sieciowych.

1. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
2. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
3. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach

zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,

1. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
2. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
3. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
4. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
5. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno

za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:

* Dropbox,
* Google Drive,
* SharePoint,
* OneDrive Business,
* OneDrive Personal.

1. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
2. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
3. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości  oraz wirtualnego drukowania,
4. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
5. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
6. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
7. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
8. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę

klasyfikacji na niższą.

1. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających

urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e- mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być

wykorzystywane do określenia reguł dostępu.

1. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz

folderów synchronizacji z usługami chmury.

1. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
2. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
3. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników

wymiennych musi być w pełni niezauważalna dla użytkownika.

1. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do

zaszyfrowanych dysków oraz dysków wymiennych.

1. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
2. numery kart kredytowych,
3. numer PESEL,
4. numer polskiego dowodu osobistego,
5. polski numer paszportu,
6. wyrażenia regularne,
7. określone ciągi znaków,
8. numer IBAN.
9. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
10. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
11. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
12. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
13. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
14. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
15. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
16. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do

rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.

1. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
2. audyt i logowanie wiadomości e-mail,
3. audyt i logowanie operacji na plikach,
4. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
5. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
6. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
7. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
8. Bezpieczeństwo danych:

* Przegląd informacji o incydentach bezpieczeństwa.
* Przegląd danych przychodzących.
* Przegląd danych wychodzących.
* Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
* Podłączane/odłączane urządzenia przenośne.

1. Produktywność:

* Przegląd informacji na temat produktywności użytkowników.
* Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
* Trendy.

1. Eksploatacja sprzętu:

* Przegląd informacji na temat eksploatacji sprzętu komputerowego.
* Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
* Eksploatacja drukarek.
* Eksploatacji sieci.

1. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
2. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
3. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera

informacje nt:

* plików przenoszonych na nośniki USB i inne urządzenia przenośne,
* plików przesłanych za pomocą wiadomości e-mail,
* plików przesłanych za pomocą poczty webowej,
* plików przesłanych do Internetu,
* plików wysłanych za pomocą komunikatorów,
* plików przesłanych na dyski chmurowe,
* analiza sposobu korzystania z aplikacji,
* analiza korzystania z Internetu,
* analiza wykorzystania porali do poszukiwania pracy.

1. **Oprogramowanie do wykonywania kopii zapasowych – 5 licencji uniwersalnych.**

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum 12 miesięcy.

|  |  |
| --- | --- |
| **Lp.** | **Minimalne wymagania Zamawiającego** |
| 1. **Wymagania ogólne** | |
|  | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, |
|  | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| 1. **Całkowite koszty posiadania** | |
|  | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
|  | Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
|  | Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. |
|  | Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
|  | Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. |
|  | Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |
|  | Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. |
|  | Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
|  | Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) |
|  | Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
|  | Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
|  | Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
|  | Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
|  | Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
|  | Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
|  | Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| 1. **Wymagania RPO** | |
|  | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
|  | Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
|  | Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. |
|  | Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
|  | Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. |
|  | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
|  | Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
|  | Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
|  | Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
|  | Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
|  | Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
|  | Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
|  | Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
|  | Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| 1. **Wymagania RTO** | |
|  | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |
|  | Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
|  | Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |
|  | Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
|  | Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
|  | Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
|  | Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
|  | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
|  | Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM |
|  | Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
|  | Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| 1. **Ograniczenie ryzyka** | |
|  | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
|  | Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |
|  | Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
|  | Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
|  | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| 1. **Środowiska fizyczne** | |
|  | Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
|  | Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
|  | Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE |
|  | Rozwiązanie musi wspierać system operacyjny macOS |
|  | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
|  | Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
|  | Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
|  | Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów |
|  | Rozwiązanie musi wspierać backup podłączonych dysków USB |
|  | Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
|  | Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) |
|  | Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
|  | Rozwiązanie musi wspierać kontrolę pasma sieciowego |
|  | Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
|  | Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
|  | Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
|  | Rozwiązanie musi wspierać technologię BitLocker |
|  | Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
|  | Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych |
|  | Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
|  | Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. |
|  | Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform |
|  | Rozwiązanie musi wspierać szyfrowanie |
|  | Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
|  | Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
|  | Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
|  | Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| 1. **Monitoring** | |
|  | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
|  | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
|  | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
|  | System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
|  | System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
|  | System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
|  | System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
|  | System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
|  | System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
|  | System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
|  | System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
|  | System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
|  | System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
|  | System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
|  | System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
|  | System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
|  | System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |
| 1. **Raportowanie** | |
|  | System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
|  | System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
|  | System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. |
|  | System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V |
|  | System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF |
|  | System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |
|  | System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |
|  | System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |
|  | System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |
|  | System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |
|  | System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |
|  | System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |
|  | System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |
|  | System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |
|  | System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
|  | System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |
|  | System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

1. **Wdrożenie systemów teleinformatycznych**

**Wdrożenie klastra serwerów**

Krok 1: Planowanie i Przygotowanie

* Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
* Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
* Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
* Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji

* Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
* Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra

* Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
* Dodanie pozostałych węzłów klastra do konfiguracji.
* Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra

* Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
* Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

* Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
* Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
* Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie

* Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
* Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
* Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

Usługi wdrożeniowe realizowane będą hybrydowo, częściowo w siedzibie Zamawiającego, częściowo przy pomocy zdalnego połączenia z systemami Zamawiającego.

1. **Wdrożenie kontrolera domeny (AD)**

Etap 1: Analiza Wstępna i Planowanie Wdrożenia

1.1. Analiza Stanu Obecnego:

* Ocena istniejącej infrastruktury IT, w tym systemów operacyjnych, sieci, aplikacji i baz danych.
* Identyfikacja istniejących rozwiązań zarządzania tożsamościami i bezpieczeństwem oraz ich ewentualnych ograniczeń.

1.2. Wymagania Organizacyjne i Techniczne:

* Konsultacje z interesariuszami w celu zrozumienia potrzeb biznesowych i oczekiwań dotyczących infrastruktury IT.
* Identyfikacja wymagań dotyczących zarządzania tożsamościami użytkowników, zasobami sieciowymi i politykami bezpieczeństwa.

1.3. Opracowanie Planu Wdrożenia:

* Sporządzenie szczegółowego planu projektowego uwzględniającego harmonogram, zadania, zasoby i odpowiedzialności.
* Określenie struktury domen, schematu nazewnictwa i strategii replikacji dla środowiska Active Directory.

Etap 2: Instalacja i Konfiguracja Środowiska Active Directory

2.1. Instalacja Roli AD DS:

* Konfiguracja serwera Windows Server jako kontrolera domeny, włączając rolę Active Directory Domain Services.

2.2. Konfiguracja DNS:

* Ustawienie serwera DNS zgodnie z wymaganiami Active Directory.
* Konfiguracja strefy forward i reverse DNS dla domeny.

2.3. Tworzenie Dominy lub Integracja:

* Utworzenie nowej domeny Active Directory lub integracja z istniejącymi domenami w środowisku.

2.4. Konfiguracja Zasad Replikacji:

* Określenie i skonfigurowanie zasad replikacji między kontrolerami domeny w różnych lokalizacjach.

Etap 3: Strukturyzacja i Organizacja Domeny

3.1. Projektowanie Struktury Organizacyjnej:

* Tworzenie jednostek organizacyjnych (OU) odpowiadających strukturze organizacyjnej firmy.
* Utworzenie kont użytkowników, grup i zasobów oraz ich odpowiednie uporządkowanie w hierarchii.

3.2. Konfiguracja Polityk Grupowych (GPO):

* Ustanowienie zasad dostępu, konfiguracji użytkowników i komputerów za pomocą GPO.
* Implementacja polityk bezpieczeństwa dotyczących haseł, dostępu i innych ustawień

Etap 4: Zabezpieczenie Active Directory

4.1. Wdrożenie Zaawansowanych Mechanizmów Zabezpieczeń:

* Konfiguracja zasad kont haseł, polityk blokowania kont, kontroli dostępu.
* Implementacja szyfrowania komunikacji i audytu zdarzeń w AD.

4.2. Konfiguracja Środków Obronnych:

* Wdrożenie mechanizmów zabezpieczeń przed atakami, w tym monitorowanie logów, wykrywanie zagrożeń i zapobieganie atakom.

Etap 5: Walidacja i Optymalizacja Konfiguracji

5.1. Testowanie Funkcjonalności i Bezpieczeństwa:

* Przeprowadzenie testów weryfikujących działanie i bezpieczeństwo środowiska AD.
* Identyfikacja i rozwiązywanie ewentualnych problemów lub luk w zabezpieczeniach.

5.2. Optymalizacja Wydajności:

* Optymalizacja konfiguracji AD w celu zapewnienia efektywności i wydajności działania.
* Integracja z istniejącymi systemami i aplikacjami w celu zapewnienia spójności działań.

Etap 6: Dokumentacja Techniczna

6.1. Sporządzenie Dokumentacji:

* Przygotowanie szczegółowej dokumentacji technicznej, zawierającej opisy konfiguracji, ustawień polityk, procedur bezpieczeństwa i architektury systemu.
* Dokumentacja będzie służyć jako punkt odniesienia dla administratorów IT i personelu technicznego.

Cel Końcowy Usługi

Finalizacja usługi zapewni pełne wdrożenie systemu Active Directory, skonfigurowane zgodnie z najlepszymi praktykami branżowymi, gotowe do efektywnego zarządzania środowiskiem IT. System będzie przygotowany do zapewnienia wysokiego poziomu bezpieczeństwa, stabilności operacyjnej i skalowalności, odpowiadając na bieżące oraz przyszłe potrzeby organizacji.

1. **Wdrożenie oprogramowania przeciwdziałającemu wyciekowi danych**

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

1. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
2. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
3. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
4. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
5. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
6. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
7. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
8. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
9. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
10. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

* Numery kart kredytowych
* Numery IBAN
* Numery dowodów osobistych
* Polski numer paszportu
* Numer PESEL

1. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
2. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
3. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
4. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
5. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
6. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
7. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

1. **Wdrożenie systemów teleinformatycznych**

Wdrożenie oprogramowania do wykonywania kopii zapasowych:

1: Planowanie i Przygotowanie

* Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
* Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
* Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2: Instalacja i Konfiguracja

* Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
* Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
* Konfiguracja połączenia ze swoim środowiskiem wirtualizacji

3: Konfiguracja Backupu

* Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
* Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
* Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4: Konfiguracja Replikacji (opcjonalnie)

* Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
* Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie

* Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
* Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6: Monitorowanie i Administracja

* Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
* Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

1. **Testy penetracyjne**

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.

Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

* wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
* skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
* weryfikacje domyślnych haseł według zadanego słownika;
* skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
* ustawienia harmonogramu skanowań;
* możliwość porównania wyników poszczególnych skanowań;
* możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
* możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

* przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
* przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
* dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
* wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
* tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
* precyzyjna konfiguracja reguł przechwytywania wiadomości;
* możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
* pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
* żądania i odpowiedzi dostępne w edytorze http;
* narzędzie do ręcznej edycji i ponownego wstawiania żądań;
* narzędzie do analizy statystycznej tokenów sesji;
* możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz  powrót do zapisanego miejsca;
* biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
* możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
* skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
* możliwość analizy docelowej aplikacji internetowych.
* narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych.  Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
2. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
3. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
4. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
5. Sprawdzenie występowania w wyciekach znalezionych loginów.
6. Enumeracja zasobów.
7. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
8. Skanowanie publicznej infrastruktury.
9. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
10. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
11. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
12. Eksploitacja.
13. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
14. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
15. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
16. Eskalacja uprawnień.
17. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
18. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
19. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.
2. Opis zakresu wykonanych prac.
3. Wyłączenia z testów jeżeli były.
4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
6. Szczegółowy opis znalezionych podatności.
7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

1. **Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami**

1. Przygotowanie kampanii socjotechnicznej;
2. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
3. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
4. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
5. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).
6. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
7. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
8. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
9. wygenerowanie niezbędnych certyfikatów SSL;
10. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);
11. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
12. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
13. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary”).
14. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
15. Wykonanie raportu z testu socjotechnicznego w języku polskim.
16. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:
17. wprowadzenie do cyberbezpieczeństwa:

* czym jest cyberbezpieczeństwo;
* dlaczego cyberbezpieczeństwo jest ważne;
* kluczowe zagadnienia związane z cyberbezpieczeństwem;
* przegląd statystyk i trendów w cyberbezpieczeństwie.

1. typy zagrożeń w cyberprzestrzeni:

* malware (wirusy, trojany, robaki itp.);
* ataki typu phishing i spear phishing;
* ataki DDoS;
* ataki ransomware;
* zagrożenia związane z sieciami społecznościowymi.

1. zasady bezpieczeństwa i praktyki:

* zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
* zasady bezpieczeństwa e-mail;
* bezpieczeństwo w sieciach bezprzewodowych;
* bezpieczne przeglądanie internetu;
* backup i odzyskiwanie danych.

1. reagowanie na incydenty i planowanie awaryjne:

* jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
* zasady reagowania na incydenty;
* planowanie awaryjne i kontynuacja działalności;
* Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

1. **Szkolenie z cyberbezpieczeństwa dla pracowników**

**Szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa**

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.

Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

1. wprowadzenie do cyberbezpieczeństwa:

* czym jest cyberbezpieczeństwo;
* dlaczego cyberbezpieczeństwo jest ważne;
* kluczowe zagadnienia związane z cyberbezpieczeństwem;
* przegląd statystyk i trendów w cyberbezpieczeństwie.

1. typy zagrożeń w cyberprzestrzeni:

* malware (wirusy, trojany, robaki itp.);
* ataki typu phishing i spear phishing;
* ataki DDoS;
* ataki ransomware;
* zagrożenia związane z sieciami społecznościowymi.

1. zasady bezpieczeństwa i praktyki:

* zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
* zasady bezpieczeństwa e-mail;
* bezpieczeństwo w sieciach bezprzewodowych;
* bezpieczne przeglądanie internetu;
* backup i odzyskiwanie danych.

1. reagowanie na incydenty i planowanie awaryjne:

* jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
* zasady reagowania na incydenty;
* planowanie awaryjne i kontynuacja działalności;
* Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Przewiduje się, że szkolenie potrwa łącznie minimum 16 godzin roboczych, rozłożonych na co najmniej 2 dni. Zajęcia będą organizowane w grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

1. **Szkolenie z cyberbezpieczeństwa dla pracowników IT/Sec**

**Szkolenie dla pracowników IT w zakresie cyberbezpieczeństwa**

Przedmiotem zamówienia jest przeprowadzenie szkolenia  z zakresu cyberbezpieczeństwa:

Szkolenie z cyberbezpieczeństwa dla pracowników IT.

Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:

* Czym jest cyberbezpieczeństwo?
* Dlaczego cyberbezpieczeństwo jest ważne?
* Kluczowe zagadnienia związane z cyberbezpieczeństwem.
* Przegląd statystyk i trendów w cyberbezpieczeństwie.

1. Typy zagrożeń w cyberprzestrzeni:

* Malware (wirusy, trojany, robaki itp.)
* Ataki typu phishing i spear phishing
* Ataki DDoS
* Ataki ransomware
* Zagrożenia związane z sieciami społecznościowymi.

1. Zasady bezpieczeństwa i praktyki:

* Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
* Zasady bezpieczeństwa e-mail
* Bezpieczeństwo w sieciach bezprzewodowych
* Bezpieczne przeglądanie internetu
* Backup i odzyskiwanie danych

1. Bezpieczeństwo systemów i sieci

* Zasady bezpieczeństwa systemów operacyjnych
* Bezpieczeństwo sieci i firewall
* Wprowadzenie do VPN
* Bezpieczeństwo urządzeń IoT
* Bezpieczeństwo w chmurze

1. Reagowanie na incydenty i planowanie awaryjne

* Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
* Zasady reagowania na incydenty
* Planowanie awaryjne i kontynuacja działalności
* Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione

1. Aktualne trendy i przyszłość cyberbezpieczeństwa

* Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
* Kryptografia i blockchain
* Bezpieczeństwo danych w erze Big Data
* Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Przewiduje się, że szkolenie potrwa łącznie minimum 16 godzin roboczych, rozłożonych na co najmniej 2 dni. Zajęcia będą organizowane w grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

1. **Szkolenie z cyberbezpieczeństwa dla menadżerów**

**Zaawansowane Szkolenie z Cyberbezpieczeństwa dla Kadry Zarządzającej**

**Cel szkolenia:**

Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

**Struktura programu szkoleniowego:**

Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.    
    
W ramach przeprowadzonego szkolenia wykonawca

**1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:**

- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.

- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

**2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:**

- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma  50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).  

- Omówienie znaczenia powyższych norm i ich  w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.

- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

* ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
* ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
* zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
* akceptowalna polityka szyfrowania SANS;
* techniki kryptograficzne - ENISA ;
* ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

**3. Omówienie zaawansowanych strategii ochrony organizacji:**

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.

-  Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.

- Szczegółowy opis i kroki zarządzania incydentami:

* wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
* rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
* analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
* klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
* priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
* podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
* ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.

- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:

* **Priorytet krytyczny** - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
* **Priorytet wysoki** - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
* **Priorytet średni** - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.

- Lista omówionych kompetencji w szkoleniu:

* Szef działu bezpieczeństwa (kierownik, dyrektor);
* Pełnomocnik ds. Bezpieczeństwa Informacji;
* Specjalista ds. Zarządzania Ryzykiem;
* Specjalista ds. Zgodności;
* Specjalista ds. Bezpieczeństwa Fizycznego;
* Architekt Systemów Bezpieczeństwa;
* Koordynator Programu Bezpieczeństwa;
* Analityk Bezpieczeństwa (II linia wsparcia);
* Inżynier ds. Bezpieczeństwa (II linia wsparcia);
* Administrator Systemów Bezpieczeństwa (II linia wsparcia);
* Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
* Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
* Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

**4. Regulacje prawne i compliance:**

- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.

- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.

- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.

- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.

- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.

- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.

- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.

- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.

- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).

- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.

- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.

- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.

- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

**5. Zarządzanie bezpieczeństwem w praktyce:**

- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

* Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
* Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
* Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
* OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
* BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
* Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.

- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie podzielone jest na 2 sesje, każda sesja odbywa się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem co najmniej 4 przerw po 15 minut. Przeznaczone jest 30 minut na pytania i odpowiedzi uczestników.

1. **Szkolenie z oprogramowania przeciwdziałającemu wyciekowi danych**

Szkolenie z obsługi oprogramowania przeciwdziałającego wyciekowi danych

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego lub online dla personelu IT, w celu przekazania kompletnej wiedzy w zakresie obsługi i wykorzystania funkcji oprogramowania przeciwdziałającego wyciekowi danych, w ich codziennej pracy.

Szkolenie obejmie co najmniej następujące obszary:

* Podstawowe informacje
* Licencjonowanie
* Wspierane systemy operacyjne
* Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych
* Omówienie instalatora oprogramowania przeciwdziałającego wyciekowi danych
* Wdrożenie serwera oprogramowania przeciwdziałającego wyciekowi danych
* Wdrożenie agentów oprogramowania przeciwdziałającego wyciekowi danych
* Wdrożenie klientów oprogramowania przeciwdziałającego wyciekowi danych
* Uruchomienie modułu analitycznego
* Analiza wycieków danych
* Filtrowanie i raporty z analizy
* Uruchomienie modułu przeciwdziałającego wyciekowi danych
* Uruchomienie szyfrowania BitLockerem
* Konfiguracja dostępu do urządzeń i portów
* Interfejs webowy oprogramowania przeciwdziałającego wyciekowi danych
* Minimalne wymagania systemowe dla omawianego oprogramowania
* Instalacja oraz konfiguracja modułu webowego oprogramowania przeciwdziałającego wyciekowi danych
* Analiza zachowań
* Zarządzenie kategoriami produktywności
* Kontrola WWW i aplikacji
* Alerty, raporty i konserwacja
* Zaawansowane DLP dla oprogramowania przeciwdziałającego wyciekowi danych
* Reguły DLP – tryby polityk
* Reguły ogólne
* Reguły aplikacji
* Po co nam kategorie danych?
* Inteligentne wyszukiwanie danych osobowych
* Czym są tagi i do czego służą?
* Reguły tagowania dla aplikacji, stron oraz lokalizacji

1. **Szkolenie AD / wirtualizacja / kopie zapasowe**

**1. Szkolenie z zakresu Active Directory (AD):**

Inicjatywa szkoleniowa dedykowana Active Directory ma za zadanie zapewnić uczestnikom wszechstronne przygotowanie do efektywnego zarządzania oraz ochrony infrastruktury Active Directory, stanowiąc fundament dla bezpiecznego i zrównoważonego zarządzania tożsamościami i dostępami w sieciowych ekosystemach organizacyjnych. Program szkoleniowy został skonstruowany tak, aby objąć spektrum zagadnień, począwszy od elementarnych, aż po zaawansowane moduły:

- Ekspozycja na Architekturę Active Directory: Wstępna faza szkolenia skupia się na dogłębnym zarysie roli i kardynalnego znaczenia infrastruktury Active Directory w procesach zarządzania identyfikowalnością użytkowników oraz moderacji dostępu. Uczestnicy zostaną wprowadzeni w kompleksową architekturę AD, eksplorując jej kluczowe usługi i funkcjonalności, w tym mechanizmy uwierzytelniania, autoryzacji oraz efektywne zarządzanie zasobami.

- Podstawy Konfiguracji i Administracji Obiektami w AD: Moduł ten kładzie nacisk na praktyczne aspekty tworzenia, konfiguracji i zarządzania obiektami takimi jak użytkownicy, grupy i komputery, działającymi w obrębie środowiska AD. Uczestnicy zdobędą umiejętności w zakresie procedur dodawania, usuwania i modyfikacji obiektów, korzystając z dedykowanych narzędzi administracyjnych.

- Wprowadzenie do Mechanizmów Polityk Grupowych: Szczegółowe omówienie i analiza roli polityk grup (Group Policy) w kontekście zarządzania konfiguracją i bezpieczeństwem infrastruktury AD. Szkolenie obejmuje metodyki tworzenia, aplikacji i administrowania politykami grupowymi, ukazując ich wpływ na regulacje i konfiguracje zarówno klientów, jak i serwerów w domenie.

- Implementacja Zasad Bezpieczeństwa w AD: Dyskusja na temat strategii i metodologii wzmocnienia zabezpieczeń infrastruktury AD, obejmująca zarządzanie uprawnieniami, monitorowanie aktywności w logach oraz konfigurację polityk bezpieczeństwa. Szkolenie podkreśla praktyczne podejście do identyfikacji, reagowania oraz efektywnego rozwiązywania incydentów bezpieczeństwa.

- Strategie Ochrony AD Przed Atakami: Analiza potencjalnych zagrożeń dla infrastruktury AD oraz zapewnienie szkolenia z procedur szybkiego reagowania i odtwarzania funkcjonalności systemu w przypadku wystąpienia ataków lub innych awarii. Ten segment szkolenia jest poświęcony rozwijaniu kompetencji w zakresie przeciwdziałania zagrożeniom, przywracania systemu do stanu operacyjnego oraz zapewnienia ciągłości działania krytycznych usług.

**2. Szkolenie z zakresu zabezpieczeń wirtualizacji:**

Inicjatywa ta jest skoncentrowana na intensyfikacji świadomości oraz ekspansji umiejętności technicznych związanych z aspektami bezpieczeństwa operacyjnego w środowiskach wirtualizowanych. Program szkoleniowy został zaprojektowany tak, aby oferować kompendium wiedzy obejmujące kluczowe segmenty:

- Fundamenty Technologii Wirtualizacji: Wstępna część szkolenia dedykowana jest dogłębnemu zrozumieniu essencji technologii wirtualizacji, przybliżając uczestnikom szeroki wachlarz platform wirtualizacyjnych, w tym, lecz nie ograniczając się do, Vmware oraz Hyper-V. Uczestnicy zostaną zaznajomieni z kluczowymi funkcjami, możliwościami oraz praktycznymi zastosowaniami tych technologii w różnorodnych kontekstach biznesowych, uwydatniając ich strategiczne znaczenie dla nowoczesnych przedsiębiorstw.

- Konstrukcja, Konfiguracja i Administrowanie Maszynami Wirtualnymi: Ten moduł szkolenia skupia się na przekazaniu praktycznych wskazówek dotyczących procesów kreowania, konfiguracji oraz zarządzania wirtualnymi maszynami. Szczególny nacisk kładziony jest na procedury instalacji systemów operacyjnych, alokacji zasobów oraz konfiguracji komunikacji sieciowej, z zamiarem maksymalizacji efektywności i wydajności wirtualnych środowisk operacyjnych.

- Metodologie Ochrony Infrastruktury Wirtualizowanej: Zaawansowany segment szkolenia poświęcony jest szczegółowej analizie i implementacji technik zabezpieczających infrastrukturę wirtualizowaną. Uczestnicy zgłębią metody i narzędzia umożliwiające izolację maszyn wirtualnych, zabezpieczanie hypervisorów oraz zarządzanie sieciami wirtualnymi, z naciskiem na kluczowe procedury monitorowania zagrożeń, konfigurację zasad zapór sieciowych oraz techniki segmentacji sieci wirtualnych. Omówione zostaną również zaawansowane strategie ochrony przed złośliwym oprogramowaniem i atakami sieciowymi, mające na celu zwiększenie odporności i bezpieczeństwa całego ekosystemu wirtualnego.

**3. Szkolenie z zakresu bezpieczeństwa kopii zapasowych:**

Inicjatywa szkoleniowa skoncentrowana na bezpieczeństwie kopii zapasowych kieruje się ku dogłębnemu zrozumieniu i praktycznej maestrii w zakresie kreowania oraz administracji bezpiecznymi mechanizmami backupu danych, akcentując na kluczowych komponentach:

- Fundamenty Backupu i Jego Znaczenie w Kontekście Bezpieczeństwa IT: Inauguracyjny moduł kursu dokonuje eksplikacji kluczowych pojęć i terminologii związanej z procesem tworzenia kopii zapasowych, podkreślając ich nieodzowną rolę w kompleksowej strategii bezpieczeństwa technologii informacyjnych oraz w zapewnieniu nieprzerwanej operacyjności korporacyjnych ekosystemów. Uczestnicy zdobywają perspektywę na istotę backupów jako niezbędnej linii obrony przed incydentami, które mogą zagrozić ciągłości działania organizacji.

- Dogłębna Analiza Typologii Kopii Zapasowych: Kurs prowadzi przez szczegółowe wyjaśnienie różnorodności form backupów – od pełnych, przez przyrostowe, aż po różnicowe – oferując równocześnie pragmatyczne wytyczne dotyczące ich efektywnego planowania, konfiguracji i implementacji. Omówienie to jest kluczowe dla zrozumienia optymalnych metod zarządzania cyklem życia danych oraz dla maksymalizacji efektywności procesów backupu.

- Implementacja Nowoczesnych Rozwiązań Backupowych: Ten segment szkolenia koncentruje się na adaptacji oraz wykorzystaniu zaawansowanych technologii i oprogramowania backupowego, włączając w to systemy lokalne oraz oparte na chmurze, techniki deduplikacji danych, mechanizmy kompresji oraz szyfrowania. Przedstawione zostają najnowsze narzędzia i metodologie, które umożliwiają zwiększenie efektywności i bezpieczeństwa procesów archiwizacji danych.

- Weryfikacja Efektywności Backupu i Strategii Odtwarzania: Kurs zawiera kompleksowe instrukcje dotyczące testowania efektywności tworzonych kopii zapasowych oraz procedur przywracania danych, z naciskiem na strategie prewencji i reagowania na kryzysy takie jak ataki ransomware. Uczestnicy uzyskują wiedzę na temat kluczowych praktyk i procedur testowych, które zapewniają gotowość na scenariusze awaryjne.

- Procedury i Strategie Odzyskiwania Danych po Awarii: Finalny moduł edukacyjny zagłębia się w omówienie metodyk i praktycznych wytycznych szybkiego odzyskiwania funkcjonalności systemów po wystąpieniu incydentów. Szczególna uwaga poświęcona jest skutecznym strategiom odzyskiwania danych, które są fundamentem dla minimalizacji czasu przestoju i optymalizacji procesu odbudowy po awarii.

**Cel szkolenia:**

Podstawowym zamierzeniem niniejszego kursu szkoleniowego jest dostarczenie uczestnikom kompleksowego zestawu wiedzy teoretycznej oraz praktycznych kompetencji, które są krytyczne dla skutecznego administrowania i nadzorowania bezpieczeństwem infrastruktury technologicznej informacyjnej. Szczególny nacisk kładziony jest na głębokie zrozumienie i zarządzanie systemem Active Directory, ekosystemami wirtualizacji oraz złożonymi strategiami implementacji systemów kopii zapasowych. Celem tego szkolenia jest nie tylko przekroczenie granic czysto teoretycznego przekazu wiedzy, ale przede wszystkim rozwinięcie praktycznych umiejętności aplikacyjnych, które umożliwią uczestnikom efektywne zabezpieczanie wartościowych zasobów informatycznych przed rosnącą gamą zagrożeń cyfrowych oraz zagwarantowanie nieprzerwanej operacyjności systemów informatycznych.

Poprzez syntezę teoretycznych fundamentów z realnymi aplikacjami praktycznymi, program ma na celu wyekwipowanie uczestników w niezbędne narzędzia do identyfikacji, adekwatnej reakcji oraz neutralizacji potencjalnych zagrożeń bezpieczeństwa cyfrowego. Ponadto, kurs stawia za cel wdrożenie uczestników w głębinę najlepszych praktyk i standardów branżowych, które stanowią o kształcie profesjonalnej codziennej praktyki. Skupienie się na tych elementach ma kluczowe znaczenie dla kształtowania w uczestnikach umiejętności nie tylko reaktywnych, ale przede wszystkim proaktywnych w kontekście zarządzania ryzykiem i ochrony infrastruktury IT. W rezultacie, program szkoleniowy ma na celu przygotowanie adeptów do pełnienia roli bastionu w obronie przed zagrożeniami, promując jednocześnie kulturę bezpieczeństwa informacyjnego, która jest fundamentem dla zrównoważonego rozwoju i innowacyjności w przestrzeni technologicznej organizacji.

Szkolenie podzielone jest na 2 sesje, każda sesja odbywa się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem co najmniej 4 przerw po 15 minut. Przeznaczone jest 30 minut na pytania i odpowiedzi uczestników.

1. **Opracowanie i wdrożenie dokumentacji SZBI.**

**Cel Usługi:**

Zasadniczym zamierzeniem proponowanej usługi jest kreacja kompleksowej, szczegółowo opracowanej dokumentacji dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), która będzie w pełni zharmonizowana z międzynarodowymi normami i aktualnymi najlepszymi praktykami, przy jednoczesnym dostosowaniu do unikatowych aspektów i wymogów strukturalnych Zamawiającego. Celem jest, aby wspomniana dokumentacja służyła jako kluczowy fundament dla efektywnego implementowania, utrzymania oraz ciągłego udoskonalania SZBI, gwarantując tym samym wytrzymałość ochrony informacji wobec szerokiego spektrum potencjalnych zagrożeń oraz podnosząc poziom zaufania wśród interesariuszy.

**Zakres Usługi:**

**1. Analiza Stanu Istniejącego i Określenie Wymagań:**

- Realizacja audytu wstępnego mającego na celu szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk i obszarów wymagających usprawnienia.

- Dokładna identyfikacja i agregacja wymagań prawnych, regulacyjnych oraz biznesowych dotyczących bezpieczeństwa informacji, aby zapewnić pełną zgodność przyszłego SZBI z obowiązującymi ramami normatywnymi.

**2. Opracowanie Dokumentacji SZBI:**

- Konstrukcja polityki bezpieczeństwa informacji, która będzie definiować kierunkowe cele, zakres działania, zasady oraz zakres odpowiedzialności w ramach struktury SZBI, stanowiąc podstawę dla wszystkich dalszych działań.

- Rozwój i formalizacja procedur, instrukcji operacyjnych, wytycznych oraz innych dokumentów kluczowych dla wdrożenia i efektywnego funkcjonowania SZBI, uwzględniając przy tym specyfikę organizacyjną Zamawiającego.

**3. Weryfikacja i Walidacja Dokumentacji:**

- Krytyczny przegląd i ocena zgodności opracowanej dokumentacji z międzynarodowymi standardami, wyznacznikami branżowymi oraz oczekiwaniami Zamawiającego, mający na celu zapewnienie jej maksymalnej adekwatności i użyteczności.

- Organizacja warsztatów, konsultacji oraz sesji feedbackowych z kluczowymi stakeholderami organizacji, w celu osiągnięcia konsensusu co do finalnej formy i treści dokumentów.

**4. Wsparcie przy Wdrożeniu Dokumentacji:**

- Oferowanie doradztwa w zakresie implementacji najlepszych praktyk dotyczących wdrożenia procedur i polityk określonych w dokumentacji SZBI, z myślą o optymalizacji procesów bezpieczeństwa.

- Asystowanie w implementacji zaleceń oraz w organizacji szkoleń dla personelu, aby zapewnić im kompleksowe zrozumienie nowych procedur i polityk.

**5. Przygotowanie do Certyfikacji:**

- Dostosowanie dokumentacji do wymogów procesu certyfikacji według wybranych standardów, na przykład ISO/IEC 27001, co zapewni organizacji gotowość do podjęcia procedur weryfikacyjnych.

**Cel Końcowy Usługi:**

Finalizacja usługi zapewni Zamawiającemu kompleksową, spójną oraz w pełni funkcjonalną dokumentację SZBI, która stanie się solidnym fundamentem dla efektywnego zarządzania bezpieczeństwem informacji. Dzięki temu, organizacja uzyska dogłębne zrozumienie metod zarządzania ryzykiem, ochrony informacji oraz adaptacji do zmieniających się zagrożeń, co w konsekwencji umożliwi ciągłe doskonalenie systemu bezpieczeństwa informacji. Opracowana dokumentacja SZBI stanie się kluczowym elementem w strukturze zarządzania organizacją, zapewniając nie tylko zgodność z międzynarodowymi normami i najlepszymi praktykami, ale również dopasowanie do specyficznych wymogów i oczekiwań Zamawiającego.

Dokumentacja ta będzie również służyć jako instrukcja operacyjna dla wszystkich pracowników i zainteresowanych stron, ułatwiając zrozumienie ich ról i odpowiedzialności w kontekście bezpieczeństwa informacji. W rezultacie, wszyscy uczestnicy procesu będą mieli jasne wytyczne dotyczące sposobu postępowania, co znacznie zwiększy ogólną świadomość bezpieczeństwa w organizacji oraz efektywność wdrażanych środków ochronnych.

Takie podejście zapewni organizacji nie tylko obronę przed potencjalnymi zagrożeniami, ale także pozytywnie wpłynie na reputację wśród klientów, partnerów biznesowych oraz innych interesariuszy, budując zaufanie poprzez demonstrację zaangażowania w ochronę poufnych informacji i danych osobowych. Finalnie, kompletna i zaktualizowana dokumentacja SZBI będzie stanowić nieoceniony zasób w procesie ciągłego monitorowania, przeglądania i ulepszania procesów bezpieczeństwa, umożliwiając organizacji dynamiczne reagowanie na nowe wyzwania i zapewniając stabilność operacyjną w zmieniającym się środowisku cyfrowym.