

Lp.	Nazwa przedmiotu zamówienia	Opis techniczny	
1.	UPS z kartą sieciową do zarządzania przez serwery	Przedmiot zamówienia:	Zasilacz awaryjny UPS
		Ilość:	1 sztuka
		Okres gwarancji producenta min.:	36 m-cy
		Obudowa	Uniwersalna tower/rack max. 2U
		Moc, napięcia, gniazda, ochrony, dodatkowe dane	Moc pozorna: 3000 VA Moc rzeczywista: 3000 W Współczynnik mocy: 1 Topologia (klasyfikacja IEC 62040-3): line-interactive Liczba, typ gniazd wyjściowych: 8 x C13, 2 x C19 Typ gniazda wejściowego: Gniazdo C20 Czas podtrzymania dla 100% obciążenia: 3 minuty Napięcie znamionowe: 230 V Tolerancja napięcia prostownika: 160 - 294 V (regulowana do 150 - 294 V) Częstotliwość znamionowa: 50/60 Hz autodetekcja Tolerancja częstotliwości: 47 - 70 Hz (system 50 Hz); 56,5 - 70 Hz (system 60 Hz); 40 Hz w trybie niskiej czułości Napięcie znamionowe wyjściowe: 230 V (domyślnie) / 200/208/220/240 V Częstotliwość wyjściowa: 50/60 Hz Baterie wymieniane przez użytkownika "na gorąco": Tak Ochrona przed przeładowaniem: Tak Ochrona przed głębokim rozładowaniem: Tak Okresowy automatyczny test baterii: Tak Zimny start: Tak Max. wymiary UPS (szer. x gł. x wys. w mm): 438 x 603 x 85,5 Poziom hałasu w odl. 1m: < 45 dBA
		System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
		Interfejs komunikacyjny	USB, RS232 DB-9 żeński (HID), miniport wyłącznik awaryjny RPO, miniport wyłącznik ON/OFF, listwa zaciskowa dla przekaźnika wyjściowego
		Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS'a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)
		Przyciski sterujące i wskaźniki diodowe LED	Poziomy rząd przycisków sterowania; Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony); Pasek LED sygnalizujący stan; sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie); przycisk Escape (anulowanie); przyciski funkcyjne (przewijanie w górę i w dół); przycisk Enter (potwierdzający)
		Wypożażenie	UPS 3 kVA, instrukcja obsługi, instrukcja bezpieczeństwa; przewód zasilający; kabel RS232; kabel USB; karta SNMP; uchwyty kablowe; podstawki do montażu pionowego (wieża); 2 przewody IEC 10 A; zestaw szyn montażowych do szafy 19" Karta SNMP "cyberbezpieczeństwo (certyfikaty UL 2900-2-2 /IEC62443 /HTTPS/MQTT/NDIS/LDAP/NVD//SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256)"; certyfikaty CA i PKI; prędkość gigabitowa (half-duplex, full-duplex); różne poziomy nadawania dostępu do konta administratora lub użytkownika
		Dołączone oprogramowanie	Oprogramowanie z subskrypcją na co najmniej 1 rok wsparcia technicznego oraz aktualizacji dla co najmniej 3 węzłów.  Oferowane oprogramowanie musi spełnić następujące warunki: <ul style="list-style-type: none"><li>• Serwer zarządzający winien występować w postaci maszyny wirtualnej dla systemów VMware, Microsoft Hyper-V, Oracle Virtual Box</li><li>• Podgląd statusu i parametrów infrastruktury zasilania i IT z poziomu jednej centralnej konsoli zarządzającej</li><li>• Integracja z systemami Vmware, Microsoft Windows Server, Nutanix, Linux, Kubernetes</li></ul>

			<ul style="list-style-type: none"><li>• Integracja z LDAP lub Active Directory</li><li>• Tworzenie wielu kont administratorów</li><li>• Komunikacja z urządzeniami zasilania poprzez protokoły takie jak: MQTT, SNMPv1/v3</li><li>• Monitorowanie dowolnego urządzenia zasilania (UPS, PDU) zgodnego z protokołem SNMP.</li><li>• Sterowanie gniazdami oraz podgląd parametrów pracy dla listew PDU</li><li>• Wizualizacja danych i parametrów urządzeń zasilania, danych z czujników środowiskowych z poziomu jednej konsoli</li><li>• Alarmowanie na podstawie parametrów takich jak: asymetria międzyfazowa, napięcie wejściowe, napięcie wyjściowe, poziom baterii w UPS, obciążenie, temperatura, wilgotność dla całego środowiska, PDU, UPS, szaf IT</li><li>• Graficzna reprezentacja monitorowanej serwerowni, szaf IT, urządzeń IT, urządzeń zasilania</li><li>• Możliwość tworzenia wielu wirtualnych serwerowni</li><li>• Generowanie wirtualnej szafy IT włącznie z parametrami konsumpcji zasilania w korelacji gniazdo-urządzenie</li><li>• Graficzna reprezentacja połączeń: urządzenie - gniazdo PDU</li><li>• Podgląd statusu maszyn wirtualnych z jednej konsoli</li><li>• Aktualizacja firmware dla UPS, PDU i kart sieciowych wbudowanych w UPS dla dedykowanych rozwiązań</li><li>• Możliwość masowej konfiguracji UPS dla dedykowanych rozwiązań</li><li>• Podgląd raportów zasilania i parametrów pracy UPS, PDU, ATS w formie wykresów</li><li>• Możliwość exportu danych w postaci pliku csv i syslog</li><li>• Powiadomienia w formie email i sms (z wykorzystaniem bramki sms)</li><li>• Możliwość tworzenia własnej treści email</li><li>• Tworzenie dynamicznych grup urządzeń fizycznych i wirtualnych w oparciu o nazwę, tag, lokalizację, kontakt, adres sieciowy</li><li>• Polityka automatyzacji budowana w centralnej konsoli zarządzającej</li><li>• Budowanie polityk automatyzacji wyłączania/włączania/migrowania dla maszyn wirtualnych, bazując na parametrach UPS.</li><li>• Możliwość budowania polityki automatyzacji w oparciu o parametry środowiskowe (temperatura, wilgotność)</li><li>• Budowanie polityki automatyzacji przy wykorzystaniu skryptów i komend poprzez protokół SSH</li><li>• Budowanie polityk automatyzacji dla klastrów serwerów</li><li>• Budowanie polityk automatyzacji dla systemów macierzy dyskowych i NAS</li><li>• Definiowanie zaawansowanych polityk automatyzacji polegających na zagnieżdżaniu elementów takich jak warunki i akcje</li><li>• Implementowanie w polityce automatyzacji akcji w postaci opóźnień bazujących na czasie, poziomie naładowania baterii, czasie podtrzymania</li><li>• Każdorazowo, przed wykonaniem akcji winno nastąpić sprawdzenie warunku początkowego polityki automatyzacji</li></ul>
		Zgodność z normami UE	Deklaracja zgodności producenta
		Dodatkowe certyfikaty	ISO9001 producenta urządzenia

2.	urządzenie UTM z licencją na 1 rok	Przedmiot zamówienia:	UTM wraz ze wsparciem oraz licencją na 1 rok
		Ilość:	1 sztuka
		Okres gwarancji producenta min.:	12 miesięcy
		Wymagania Ogólne	<p>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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall.</li> <li>• Ochrony w warstwie aplikacji.</li> <li>• Protokołów routingu dynamicznego.</li> </ul>
		Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> <li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastry Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> <li>4. System umożliwia agregację linków statyczną oraz w oparciu o protokoły LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych</li> </ol>
		Interfejsy, Dysk, Zasilanie:	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ol style="list-style-type: none"> <li>a. 10 portami Gigabit Ethernet RJ-45.</li> <li>b. 2 gniazdami SFP 1 Gbps.</li> </ol> </li> <li>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>3. System jest wyposażony w zasilanie AC.</li> </ol>
		Funkcje Systemu Bezpieczeństwa:	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li> <li>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.</li> <li>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</li> <li>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</li> <li>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).</li> </ol>
		Polityki, Firewall	<ol style="list-style-type: none"> <li>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje za zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ol style="list-style-type: none"> <li>a. Translację jeden do jeden oraz jeden do wielu.</li> <li>b. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ol> </li> <li>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> <li>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</li> </ol>

			<div><div>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</div><div>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</div><div>7. 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.<div><div>a. Amazon Web Services (AWS).</div><div>b. Microsoft Azure.</div><div>c. Cisco ACI.Google Cloud Platform (GCP).</div><div>d. OpenStack.</div><div>e. VMware NSX.</div><div>f. Kubernetes.</div></div></div></div>
		Połączenia VPN	<div><div>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:<div><div>a. Wsparcie dla IKE v1 oraz v2.</div><div>b. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</div><div>c. Obsługa protokołu Diffie-Hellman grup 19, 20.</div><div>d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</div><div>e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</div><div>f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</div><div>g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</div><div>h. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</div><div>i. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</div><div>j. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</div><div>k. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</div><div>l. Mechanizm „Split tunneling” dla połączeń Client-to-Site.</div></div></div><div>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:<div><div>a. 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.</div><div>b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</div><div>c. 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.</div></div></div></div>
		Routing i obsługa łączy WAN	<div><div>W zakresie routingu rozwiązanie zapewnia obsługę:</div><div><div>1. Routingu statycznego.</div><div>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</div><div>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</div><div>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</div><div>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</div><div>6. BFD (Bidirectional Forwarding Detection).</div><div>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</div></div></div>
		Funkcje SD-WAN	<div><div>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</div><div>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</div></div>
		Zarządzanie pasmem	<div><div>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</div><div>2. System daje możliwość określenia pasma dla poszczególnych aplikacji.</div><div>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</div><div>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</div></div>
		Ochrona przed malware	<div><div>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</div><div>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</div><div>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.</div><div>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</div><div>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</div><div>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div><div>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.</div><div>8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</div><div>9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.</div></div>

			10.   Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
	Ochrona przed atakami		<ol style="list-style-type: none"><li>1.   Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</li><li>2.   System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</li><li>3.   Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</li><li>4.   System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li><li>5.   Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</li><li>6.   Możliwość kontrolowania długości nagłówka, ilości parametrów URL   oraz Cookies dla protokołu http.</li><li>7.   Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</li><li>8.   Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</li></ol>
	Kontrola aplikacji		<ol style="list-style-type: none"><li>1.   Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</li><li>2.   Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</li><li>3.   Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</li><li>4.   Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</li><li>5.   Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</li><li>6.   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).</li></ol>
	Kontrola WWW		<ol style="list-style-type: none"><li>1.   Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL   pogrupowanych w kategorie tematyczne.</li><li>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.</li><li>3.   Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</li><li>4.   Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</li><li>5.   Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</li><li>6.   Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</li><li>7.   Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</li><li>8.   Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</li><li>9.   System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</li></ol>
	Uwierzytelnianie użytkowników w ramach sesji		<ol style="list-style-type: none"><li>1.   System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none"><li>•   Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li><li>•   Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li><li>•   Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li></ul></li><li>2.   System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</li><li>3.   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.</li><li>4.   Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</li></ol>
	Zarządzanie		<ol style="list-style-type: none"><li>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.</li><li>2.   Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest   realizowana z wykorzystaniem szyfrowanych protokołów.</li><li>3.   Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</li><li>4.   System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</li><li>5.   System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</li><li>6.   Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</li><li>7.   Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</li><li>8.   Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</li><li>9.   Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</li></ol>
	Logowanie		<ol style="list-style-type: none"><li>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.</li><li>2.   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.</li><li>3.   Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</li><li>4.   Możliwość włączenia logowania per reguła w polityce firewall.</li><li>5.   System zapewnia możliwość logowania do serwera SYSLOG.</li><li>6.   Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</li></ol>

		<table><tr><td>Serwisy i licencje</td><td>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 24 miesięcy.</td></tr><tr><td>Gwarancja oraz wsparcie</td><td>System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.</td></tr></table>	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 24 miesięcy.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.														
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 24 miesięcy.																			
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.																			
3.	switch klasy enterprise z licencjami na 1 rok, 48 portów POE	<table><tr><td>Przedmiot zamówienia:</td><td>Switch klasy enterprise z licencjami na 1 rok, 48 portów POE</td></tr><tr><td>Ilość:</td><td>1 sztuka</td></tr><tr><td>Okres gwarancji producenta min.:</td><td>12 miesięcy</td></tr><tr><td colspan="2">Parametry</td></tr><tr><td>Przełącznik sieciowy</td><td>W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.</td></tr><tr><td>Parametry fizyczne platformy</td><td><ul style="list-style-type: none"><li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li><li>Zasilanie AC 230V.</li></ul></td></tr><tr><td>Interfejsy sieciowe - wymagania minimalne</td><td>1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:<ul style="list-style-type: none"><li>48 porty GE RJ-45.</li><li>4 porty 10 GE SFP+.</li></ul></td></tr><tr><td>Zarządzanie</td><td><ul style="list-style-type: none"><li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li><li>Wsparcie dla SNMP w wersjach 1-3</li><li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li><li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li><li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li><li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li><li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li><li>Automatycznie wykonywane rewizje konfiguracji.</li></ul></td></tr><tr><td>Wymagane funkcje</td><td><ul style="list-style-type: none"><li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>Obsługa Jumbo Frames.</li><li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>Agregacja portów zgodna ze standardem 802.3ad.</li><li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>Port-mirroring.</li></ul></td></tr></table>	Przedmiot zamówienia:	Switch klasy enterprise z licencjami na 1 rok, 48 portów POE	Ilość:	1 sztuka	Okres gwarancji producenta min.:	12 miesięcy	Parametry		Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.	Parametry fizyczne platformy	<ul style="list-style-type: none"><li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li><li>Zasilanie AC 230V.</li></ul>	Interfejsy sieciowe - wymagania minimalne	1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ul style="list-style-type: none"><li>48 porty GE RJ-45.</li><li>4 porty 10 GE SFP+.</li></ul>	Zarządzanie	<ul style="list-style-type: none"><li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li><li>Wsparcie dla SNMP w wersjach 1-3</li><li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li><li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li><li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li><li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li><li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li><li>Automatycznie wykonywane rewizje konfiguracji.</li></ul>	Wymagane funkcje	<ul style="list-style-type: none"><li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>Obsługa Jumbo Frames.</li><li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>Agregacja portów zgodna ze standardem 802.3ad.</li><li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>Port-mirroring.</li></ul>
Przedmiot zamówienia:		Switch klasy enterprise z licencjami na 1 rok, 48 portów POE																		
Ilość:		1 sztuka																		
Okres gwarancji producenta min.:		12 miesięcy																		
Parametry																				
Przełącznik sieciowy		W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.																		
Parametry fizyczne platformy		<ul style="list-style-type: none"><li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li><li>Zasilanie AC 230V.</li></ul>																		
Interfejsy sieciowe - wymagania minimalne		1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ul style="list-style-type: none"><li>48 porty GE RJ-45.</li><li>4 porty 10 GE SFP+.</li></ul>																		
Zarządzanie		<ul style="list-style-type: none"><li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li><li>Wsparcie dla SNMP w wersjach 1-3</li><li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li><li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li><li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li><li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li><li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li><li>Automatycznie wykonywane rewizje konfiguracji.</li></ul>																		
Wymagane funkcje	<ul style="list-style-type: none"><li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>Obsługa Jumbo Frames.</li><li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>Agregacja portów zgodna ze standardem 802.3ad.</li><li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>Port-mirroring.</li></ul>																			

			<ul style="list-style-type: none"><li>• Uwierzytelnianie 802.1x na poziomie portu.</li><li>• Uwierzytelnianie 802.1x w oparciu o adres MAC.</li><li>• W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li><li>• W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li><li>• W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li></ul>
		Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"><li>1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:<ul style="list-style-type: none"><li>• Centralne zarządzanie konfiguracją urządzenia</li><li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li><li>• Centralne zarządzanie sieciami VLAN.</li><li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li><li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li><li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li><li>• Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.</li><li>• Automatyczna detekcja i rekomendacje konfiguracji.</li><li>• Przesyłanie logów na zewnętrzny serwer syslog.</li><li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li><li>• Obsługa białych i czarnych list adresów MAC.</li><li>• Wykrywanie aplikacji komunikujących się w sieci.</li></ul></li><li>2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</li><li>3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.</li></ol>
		Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"><li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li><li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li></ul>
		Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.
4.	punkt dostępowy sieci bezprzewodowej	Przedmiot zamówienia:	Punkt dostępowy sieci bezprzewodowej z licencjami na 1 rok
		Ilość:	2 sztuki
		Okres gwarancji producenta:	12 miesięcy

	z licencjami na 1 rok	Parametry	
		Opis	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
		Dane techniczne	<ol style="list-style-type: none"> <li>Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: <ol style="list-style-type: none"> <li>Temperatura 0–50°C,</li> <li>Wilgotność 5–90%.</li> </ol> </li> <li>Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.</li> <li>Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy: <ol style="list-style-type: none"> <li>2.4 GHz 802.11b/g/n,</li> <li>5 GHz 802.11a/n/ac/ax,</li> <li>6 GHz 802.11ax/be</li> </ol> </li> <li>Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.</li> <li>Urządzenie musi być wyposażone w moduł BLE.</li> <li>Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.</li> <li>Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.</li> <li>Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: <ol style="list-style-type: none"> <li>Tunnel,</li> <li>Bridge,</li> <li>Mesh.</li> </ol> </li> <li>Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.</li> <li>Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist &amp; whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).</li> <li>Interfejs radiowy urządzenia powinien wspierać następujące funkcje: <ol style="list-style-type: none"> <li>MIMO – 2x2,</li> <li>Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych: <ol style="list-style-type: none"> <li>688 Mbps;</li> <li>2882 Mbps;</li> <li>5765 Mbps;</li> </ol> </li> <li>Wymagana moc nadawania: <ol style="list-style-type: none"> <li>min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;</li> </ol> </li> </ol> </li> </ol>



			<div>ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;</div> <div>iii. min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm</div> <div>d. Wsparcie dla kanałów 20/40/80/160/320MHz,</div> <div>e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.</div> <div>f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.</div> <div>g. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.</div> <div>12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512</div> <div>13. Funkcje dodatkowe:<div>a. OFDMA UL i DL</div><div>b. Spatial Reuse (BSS Coloring)</div><div>c. UL-MU-MIMO</div><div>d. DL-MU-MIMO</div><div>e. Enhanced Target Wake Time (TWT)</div><div>f. Wbudowany analizator widma</div><div>a. Wbudowane mechanizmy WIPS/WIDS</div></div>
		Gwarancja oraz wsparcie	Urządzenie musi mieć zapewnioną dożywną ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.
5.	serwer	<div>Przedmiot zamówienia:</div> <div>Ilość:</div> <div>Okres gwarancji min.:</div> <div>Obudowa</div> <div>Płyta główna</div> <div>Chipset</div> <div>Procesor</div>	<div>Serwer</div> <div>1 sztuka</div> <div>36 m-cy</div> <div><div><div></div><div>Obudowa Rack o wysokości max 2U z możliwością instalacji min. 16 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</div></div><div><div></div><div>Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</div></div><div>Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.</div></div> <div><div><div></div><div>Płyta główna z możliwością zainstalowania do dwóch procesorów.</div></div><div><div></div><div>Obsługa procesorów 32 rdzeniowych.</div></div><div><div></div><div>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</div></div><div><div></div><div>Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci.</div></div><div>Płyta główna powinna obsługiwać do 1TB pamięci RAM.</div></div> <div>Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych</div> <div>Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 3,9GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 291 w teście SPECrate2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej.</div>

		<b>RAM</b>	Minimum 256GB DDR5 RDIMM 4800MT/s,
		<b>Funkcjonalność pamięci RAM</b>	<ul style="list-style-type: none"><li>• Demand Scrubbing,</li><li>• Patrol Scrubbing,</li></ul> Permanent Fault Detection (PFD)
		<b>Gniazda PCI</b>	Min. trzy sloty PCIe
		<b>Kontroler RAID</b>	<ul style="list-style-type: none"><li>• Sprzętowy kontroler dyskowy, posiadający<ul style="list-style-type: none"><li>◦ Min. 8GB nieulotnej pamięci cache,</li><li>◦ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.</li></ul></li></ul> Wsparcie dla dysków samoszyfrujących
		<b>Dyski twarde</b>	<ul style="list-style-type: none"><li>• Zainstalowane:<ul style="list-style-type: none"><li>◦ 16x dysk ISE SAS o pojemności min. 1,2TB, Hot-Plug</li></ul></li></ul> Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
		<b>Interfejsy sieciowe/FC/SAS</b>	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
		<b>Wbudowane porty</b>	<ul style="list-style-type: none"><li>• 4x USB, w tym min. 1 porty USB 3.0</li><li>• 2x port VGA (jeden na panelu przednim)</li></ul> Możliwość rozbudowy o Serial Port
		<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
		<b>Wentylatory</b>	Redundantne, Hot-Plug
		<b>Zasilacze</b>	Redundantne, Hot-Plug min. 1100W klasy Titanium
		<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"><li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li><li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li><li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li><li>• Moduł TPM 2.0</li><li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li><li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li><li>• 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).</li></ul>
		<b>Karta Zarządzania</b>	<ul style="list-style-type: none"><li>• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:<ul style="list-style-type: none"><li>◦ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li><li>◦ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li><li>◦ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li><li>◦ możliwość podmontowania zdalnych wirtualnych napędów;</li><li>◦ wirtualną konsolę z dostępem do myszy, klawiatury;</li><li>◦ wsparcie dla IPv6;</li><li>◦ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li><li>◦ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li><li>◦ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li><li>◦ integracja z Active Directory;</li><li>◦ możliwość obsługi przez dwóch administratorów jednocześnie;</li><li>◦ wsparcie dla dynamic DNS;</li><li>◦ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li><li>◦ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li><li>◦ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li></ul></li></ul>

			<p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"><li>o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li><li>o Przesyłanie danych telemetrycznych w czasie rzeczywistym</li><li>o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li><li>o Automatyczna rejestracja certyfikatów (ACE)</li></ul>
		<b>Oprogramowanie do zarządzania</b>	<ul style="list-style-type: none"><li>• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:<ul style="list-style-type: none"><li>o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li><li>o integracja z Active Directory</li><li>o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li><li>o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li><li>o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li><li>o Szczegółowy opis wykrytych systemów oraz ich komponentów</li><li>o Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li><li>o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li><li>o Grupowanie urządzeń w oparciu o kryteria użytkownika</li><li>o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li><li>o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li><li>o Szybki podgląd stanu środowiska</li><li>o Podsumowanie stanu dla każdego urządzenia</li><li>o Szczegółowy status urządzenia/elementu/komponentu</li><li>o Generowanie alertów przy zmianie stanu urządzenia.</li><li>o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li><li>o Integracja z service desk producenta dostarczonej platformy sprzętowej</li><li>o Możliwość przejęcia zdalnego pulpitu</li><li>o Możliwość podmontowania wirtualnego napędu</li><li>o Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li><li>o Możliwość importu plików MIB</li><li>o Przesyłanie alertów „as-is” do innych konsol firm trzecich</li><li>o Możliwość definiowania ról administratorów</li><li>o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li><li>o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li><li>o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li><li>o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li><li>o 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.</li><li>o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li><li>o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</li><li>o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li><li>o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li><li>o Zdalne uruchamianie diagnostyki serwera.</li><li>o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li><li>o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li></ul></li></ul>
		<b>Certyfikaty</b>	<ul style="list-style-type: none"><li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li><li>• Serwer musi posiadać deklaracja CE.</li><li>• Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.</li><li>• 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 <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - <b>Wykonawca może zostać wezwany do złożenia dokumentu potwierdzającego spełnianie wymogu.</b></li><li>• 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.</li></ul>
		<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"><li>• Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li></ul>

			<ul style="list-style-type: none"><li>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li></ul>
		Warunki gwarancji	<ul style="list-style-type: none"><li>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat.</li><li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li><li>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)</li><li>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li><li>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.</li><li>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li><li>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.</li><li>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.</li><li>Zamawiający może wymagać od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</li><li>Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:<ul style="list-style-type: none"><li>Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li><li>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.</li><li>Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.</li><li>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.</li><li>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.</li></ul></li><li>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</li><li>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.</li></ul>
6.	serwer do zarządzania kopiami bezpieczeństwa	Przedmiot zamówienia:	Serwer zarządzania kopiami
		Ilość:	1 sztuka
		Okres gwarancji producenta min.:	36 m-cy
		Obudowa	<ul style="list-style-type: none"><li>tower</li></ul>
		Płyta główna	<ul style="list-style-type: none"><li>Płyta główna z możliwością zainstalowania jednego procesora.</li><li>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li><li>na płycie głównej powinny znajdować się minimum 2 sloty przeznaczonych do instalacji pamięci</li></ul>
		Procesor	<ul style="list-style-type: none"><li>Zainstalowany jeden procesor 20-rdzeniowy klasy x86, min. 2,4GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 49553 na dzień 27.10.2025 w teście PassMark dostępnym na stronie internetowej: <a href="https://www.cpubenchmark.net/">https://www.cpubenchmark.net/</a></li></ul>
		Pamięć RAM	<ul style="list-style-type: none"><li>16GB DDR5 4400 MT/s</li></ul>
		Dysk twardy	<ul style="list-style-type: none"><li>512GB SSD</li><li>10TB HDD, dedykowany do pracy ciągłej (Zamawiający dopuszcza możliwość montażu dysku producenta innego niż producent komputera)</li></ul>

		Interfejs sieciowy	<ul style="list-style-type: none"><li>1x 1GE RJ45</li></ul>
		Porty	<ul style="list-style-type: none"><li>1x USB 3.2 Gen1 Type-C</li><li>5x USB 3.2 Gen1 Type-A</li><li>4x USB 2.0</li><li>1x Audio</li><li>3x DP</li></ul>
		Zasilanie	<ul style="list-style-type: none"><li>260W PSU</li></ul>
		Warunki gwarancji	<ul style="list-style-type: none"><li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li><li>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)</li><li>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</li><li>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.</li><li>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li><li>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li><li>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</li><li>Zamawiający wymaga od podmiotu realizującego serwis, dostawę 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.</li><li>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.</li></ul>
7.	licencja na system archiwizacji maszyn wirtualnych	Przedmiot zamówienia:	Oprogramowanie do tworzenia oraz zarządzania kopiami bezpieczeństwa
		Ilość:	4 sztuki
		Okres trwania subskrypcji:	1 rok
		Wymagania ogólne	<p>Oprogramowanie z licencją umożliwiającą obciążenie w ilości 5 maszyn wirtualnych.</p> <p>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: <a href="https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions">https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions</a> i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,</p> <p>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</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.</p> <p>Całkowite koszty posiadania</p> <p>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej</p> <p>Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków</p> <p>Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej</p>

			<p>specyfikacji</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie musi wspierać niezmiennosc kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania</p> <p>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)</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji</p> <p>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</p> <p>Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania</p> <p>Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p> <p>Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej</p> <p>Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)</p> <p>Oprogramowanie musi posiadać integrację z systemami zarządzania kluczami szyfrującymi (KMS)</p> <p>Oprogramowanie musi posiadać integrację z systemami typu SIEM</p> <p>Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.</p>
		Wymagania RPO	<p>Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej</p> <p>Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>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 datastora</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewnić odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</p> <p>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.</p> <p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>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.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAI0, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</p> <p>Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</p>
		Wymagania RTO	<p>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.</p> <p>Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>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</p> <p>Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre</p>

		<p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.</p> <p>Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny.</p> <p>Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików</p> <p>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.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM</p> <p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>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</p> <p>oraz pozwalać na odtworzenie haseł.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p> <p>Ograniczenie ryzyka</p> <p>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 uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>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</p> <p>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.</p> <p>Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware</p> <p>Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania</p> <p>Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków</p> <p>Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p>	
8.	przesyłanie logów w czasie rzeczywistym i przechowywanie przez dwa lata u zewnętrznego dostawcy	Przedmiot zamówienia:	Agregacja logów
		Ilość:	12 sztuk
		Okres świadczenia usługi:	12 miesięcy
		Opis	Przedmiot zamówienia stanowi świadczenie usług przechowywania logów systemowych pochodzących z Kontrolera Domeny i urzędnia UTM Zamawiającego, z wykorzystaniem bezpiecznego połączenia VPN. Usługa ta ma na celu zapewnienie bezpieczeństwa oraz możliwości rozliczenia działań zgodnie z obowiązującymi wymogami prawnymi.

		Zakres usługi	Konfiguracja i zarządzanie połączeniem VPN, umożliwiające przesyłanie logów z systemów Zamawiającego do systemów IT przechowujące dane u Wykonawcy. Połączenie musi spełniać następujące kryteria:	
			<ul style="list-style-type: none"><li>Komunikacja sieciowa możliwa tylko w kierunku od Zamawiającego do Wykonawcy.</li><li>Zapobieganie inicjowaniu połączenia od Wykonawcy do Zamawiającego.</li><li>Wykluczenie możliwości routowania z VPN do wewnętrznych sieci komputerowych Zamawiającego.</li></ul>	
Zarejestrowane logi muszą zawierać szczegółowe informacje dotyczące:				
<ul style="list-style-type: none"><li>dostępu użytkowników do systemów lub zbiorów danych,</li><li>zmian w konfiguracji zabezpieczeń,</li><li>dostępu do informacji objętych ochroną prawną, zdarzeń systemowych.</li></ul>				
Przechowywanie logów przez okres co najmniej 24 miesięcy, nawet po zakończeniu świadczenia usługi. Wykonawca musi zapewnić przechowywanie wcześniej zebranych logów przez 24 miesiące od ich zebrania niezależnie od zaprzestania świadczenia usługi. Zamawiający może zażądać usunięcia zebranych logów poprzez przekazanie dokumentu podpisanego przez osobę uprawnioną.				
			Wykonawca dostarcza rozwiązania techniczne gwarantujące, zabezpieczenie logów przed edycją i nieautoryzowanym usunięciem.	
		Zgodność	Usługa musi być zgodna z:	
			<ul style="list-style-type: none"><li>Polską Normą PN-ISO/IEC 27002,</li><li>Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych</li></ul>	
9.	UPS	Przedmiot zamówienia:		UPS
		Ilość:		1 sztuka
		Okres gwarancji producenta:		36 miesięcy
		Parametry		
		Moc pozorna		700 VA
		Moc rzeczywista		420 W
		Układ ochrony przeciwprzepięciowej		Tak
		Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową		3x FR
		Liczba, typ gniazd wyj. z ochroną przepięciową		1x FR
		Typ gniazda wejściowego		IEC320 C14 (10A)
		Napięcie znamionowe wejściowego		230 V
		Tolerancja napięcia wejściowego		184 V – 264 V (regulacja 161 V – 284 V)
		Częstotliwość znamionowa		50 – 60 Hz
		Tolerancja częstotliwości		46 – 70 Hz
		Napięcie znamionowe wyjściowe		230 V (domyślnie), 220/240 V



		<table><tr><td>Baterie wymieniane przez użytkownika</td><td>Tak</td></tr><tr><td>Baterie wewnętrzne o pojemności</td><td>1 x 7Ah 12V</td></tr><tr><td>Porty komunikacji</td><td>USB, HID</td></tr><tr><td>Maksymalna szerokość</td><td>81 mm</td></tr><tr><td>Maksymalna wysokość</td><td>263 mm</td></tr><tr><td>Maksymalna wysokość</td><td>263 mm</td></tr><tr><td>Maksymalna głębokość</td><td>235 mm</td></tr><tr><td>Maksymalny ciężar</td><td>3,7 kg</td></tr><tr><td>Zimny start</td><td>Tak</td></tr><tr><td>Uruchomienie z baterii</td><td>Tak</td></tr><tr><td>Ochrona przed przeładowaniem</td><td>Tak</td></tr><tr><td>Certyfikat CE</td><td>Tak</td></tr></table>	Baterie wymieniane przez użytkownika	Tak	Baterie wewnętrzne o pojemności	1 x 7Ah 12V	Porty komunikacji	USB, HID	Maksymalna szerokość	81 mm	Maksymalna wysokość	263 mm	Maksymalna wysokość	263 mm	Maksymalna głębokość	235 mm	Maksymalny ciężar	3,7 kg	Zimny start	Tak	Uruchomienie z baterii	Tak	Ochrona przed przeładowaniem	Tak	Certyfikat CE	Tak
Baterie wymieniane przez użytkownika	Tak																									
Baterie wewnętrzne o pojemności	1 x 7Ah 12V																									
Porty komunikacji	USB, HID																									
Maksymalna szerokość	81 mm																									
Maksymalna wysokość	263 mm																									
Maksymalna wysokość	263 mm																									
Maksymalna głębokość	235 mm																									
Maksymalny ciężar	3,7 kg																									
Zimny start	Tak																									
Uruchomienie z baterii	Tak																									
Ochrona przed przeładowaniem	Tak																									
Certyfikat CE	Tak																									
10.	ups dla 3 jednostek podległych, tj. 5 dla GOPS, 5 dla CUW, 5 dla GZGKiM	Poz. 9																								
11.	program antywirusowy dla Urzędu Gminy Malbork	<table><tr><td>Przedmiot zamówienia:</td><td>Oprogramowanie antywirusowe z usługą chmurową</td></tr><tr><td>Ilość:</td><td>25 sztuk</td></tr><tr><td>Okres trwania licencji:</td><td>12 miesięcy</td></tr><tr><td>Administracja zdalna w chmurze</td><td>1.Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2.Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3.Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4.Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5.Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7.Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8.Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak. 9.Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10.Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11.Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12.Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.</td></tr><tr><td>Ochrona stacji roboczych</td><td>1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2.Rozwiązanie musi wspierać architekturę ARM64.</td></tr></table>	Przedmiot zamówienia:	Oprogramowanie antywirusowe z usługą chmurową	Ilość:	25 sztuk	Okres trwania licencji:	12 miesięcy	Administracja zdalna w chmurze	1.Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2.Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3.Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4.Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5.Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7.Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8.Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak. 9.Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10.Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11.Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12.Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.	Ochrona stacji roboczych	1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2.Rozwiązanie musi wspierać architekturę ARM64.														
Przedmiot zamówienia:	Oprogramowanie antywirusowe z usługą chmurową																									
Ilość:	25 sztuk																									
Okres trwania licencji:	12 miesięcy																									
Administracja zdalna w chmurze	1.Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2.Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3.Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4.Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5.Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7.Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8.Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnień: odczyt, użyj, zapisz oraz brak. 9.Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10.Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11.Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12.Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.																									
Ochrona stacji roboczych	1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2.Rozwiązanie musi wspierać architekturę ARM64.																									

			<p>3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4.Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</p> <p>5.Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</p> <p>6.Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>7.Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8.Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>9.Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.</p> <p>10.Rozwiązanie musi integrować się z Intel Threat Detection Technology.</p> <p>11.Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <p>12.Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>13.Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>14.Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>15.Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>16.Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> <li>•tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,</li> <li>•tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,</li> <li>•tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,</li> <li>•tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,</li> <li>•tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</li> </ul> <p>17.Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>18.Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p> <p>19.Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>20.Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>21.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>22.Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.</p> <p>23.Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none"> <li>•tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,</li> <li>•tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,</li> <li>•tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,</li> <li>•tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.</li> </ul> <p>24.Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.</p> <p>25.Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.</p> <p>26.Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>27.Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.</p> <p>28.Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.</p> <p>29.Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</p> <p>30.W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.</p>
		Ochrona serwera	<p>1.Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.</p> <p>2.Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4.Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5.Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p>

			<p>6.Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>7.Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8.Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przysyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9.Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10.Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11.Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13.Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14.Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15.Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci</p> <p>oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16.Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17.Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18.Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19.Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20.Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>21.Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.</p>
		Ochrona urządzeń mobilnych opartych o system Android	<p>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p> <p>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <p>a. usunięcie zawartości urządzenia,</p> <p>b. przywrócenie urządzenie do ustawień fabrycznych,</p> <p>c. zablokowania urządzenia,</p> <p>d. uruchomienie sygnału dźwiękowego,</p> <p>e. lokalizację GPS.</p> <p>6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</p> <p>7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p> <p>a. nazwę aplikacji,</p> <p>b. nazwę pakietu,</p> <p>c. kategorię sklepu Google Play,</p> <p>d. uprawnienia aplikacji,</p> <p>e. pochodzenie aplikacji z nieznanego źródła.</p>
12.	licencje klienckie do systemu serwerowego dla 3 jednostek podległych tj. 15 dla GOPS, 5 dla CUW, 5 dla GZGKiM	Przedmiot zamówienia:	Licencje dostępowe do serwerowego systemu operacyjnego
		Ilość:	25 sztuk
		Opis	<p>Licencja dostępowa per urządzenie dedykowana do zamawianego serwerowego systemu operacyjnego.</p> <p>Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne.</p>

13.	switch klasy enterprise z licencjami na 2 lata - 24 porty	Przedmiot zamówienia:	Switch z licencjami na 2 lata
		Ilość:	1 sztuka
		Okres gwarancji producenta min.:	12 miesięcy
		Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
		Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>Zasilanie AC 230V.</li> </ul>
		Interfejsy sieciowe	<p>Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:</p> <ul style="list-style-type: none"> <li>24 porty GE RJ-45</li> <li>4 porty 10 GE SFP+.</li> </ul>
		Zarządzanie	<ul style="list-style-type: none"> <li>Wbudowany port konsoli szeregowej do pełnego zarządzania.</li> <li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>Automatycznie wykonywane rewizje konfiguracji.</li> </ul>
		Wymagane funkcje	<ul style="list-style-type: none"> <li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>Obsługa Jumbo Frames.</li> <li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>Agregacja portów zgodna ze standardem 802.3ad.</li> <li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>Port-mirroring.</li> <li>Uwierzytelnianie 802.1x na poziomie portu.</li> <li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> </ul>

			<ul style="list-style-type: none"><li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li></ul>
		Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"><li>Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:<ul style="list-style-type: none"><li>Centralne zarządzanie konfiguracją urządzenia</li><li>Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li><li>Centralne zarządzanie sieciami VLAN.</li><li>Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li><li>Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li><li>Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li><li>Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.</li><li>Automatyczna detekcja i rekomendacje konfiguracji.</li><li>Przesyłanie logów na zewnętrzny serwer syslog.</li><li>Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li><li>Obsługa białych i czarnych list adresów MAC.</li><li>Wykrywanie aplikacji komunikujących się w sieci.</li></ul></li><li>Musi być możliwe redundantne połączenie z elementami zarządzającymi.</li><li>W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.</li></ol>
		Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"><li>System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym</li><li>System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li></ul>
		Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.
14.	licencja na serwerowy system operacyjny	Przedmiot zamówienia:	Licencja na serwerowy system operacyjny
		Ilość:	1 sztuka
		Opis licencji	Licencja na serwerowy system operacyjny która zapewni poniżej opisane funkcjonalności dla serwera posiadającego 16 rdzeni procesora. Zamawiający wymaga dostarczenia licencji imiennej (na organizację), umożliwiającej przeniesienie w ramach programu licencji zbiorczych. Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne. Nie dopuszcza się licencjonowania typu OEM (przypisanego do maszyny fizycznej).
		Minimalne parametry	<ul style="list-style-type: none"><li>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nieograniczonej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li><li>Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</li><li>Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</li><li>Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.</li><li>Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li></ul>

		<ul style="list-style-type: none"><li>• Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li><li>• Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li><li>• Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li><li>• Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</li><li>• Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li><li>• Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li><li>• Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li><li>• Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</li><li>• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li><li>• Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li><li>• Graficzny interfejs użytkownika.</li><li>• Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</li><li>• Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</li><li>• Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li><li>• Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li><li>• Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</li><li>• Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny, Zdalna dystrybucja oprogramowania na stacje robocze, Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: -dystrybucję certyfikatów poprzez http, -konsolidację CA dla wielu lasów domeny, - konsolidację CA dla wielu lasów domeny, szyfrowanie plików i folderów, Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, Serwis udostępniania stron WWW, Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</li><li>• Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: -Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych, - Obsługi 4-KB sektorów dysków, - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,</li><li>• Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,</li><li>• Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</li><li>• Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</li><li>• Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</li><li>• Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</li><li>• Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</li><li>• Sterowniki i dokumentacja od producenta sprzętu</li><li>• Oprogramowanie musi być dostarczone w najnowszej wersji</li></ul>						
15.	program antywirusowy dla jednostek podległych, tj. 15 dla GOPS, 5b dla CUW, 5 dla GZGKiM	Poz. 11						
16.	Wdrożenie UTM	<table><tr><td>Przedmiot zamówienia:</td><td>Usługa wdrożenia oraz dostosowania serwera, urządzeń sieciowych i oprogramowania zgodnie z wymogami KRI</td></tr><tr><td>Ilość:</td><td>1 sztuka</td></tr><tr><td>Wdrożenie urządzenia UTM oraz integracja z środowiskiem IT.</td><td>Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do aktualnych wersji oprogramowania. Wydzielenie podsieci VLAN w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgodnie z wymaganiami Zamawiającego. Integracja z Istniejącym środowiskiem IT. Wdrożenie VPN – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN.</td></tr></table>	Przedmiot zamówienia:	Usługa wdrożenia oraz dostosowania serwera, urządzeń sieciowych i oprogramowania zgodnie z wymogami KRI	Ilość:	1 sztuka	Wdrożenie urządzenia UTM oraz integracja z środowiskiem IT.	Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do aktualnych wersji oprogramowania. Wydzielenie podsieci VLAN w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgodnie z wymaganiami Zamawiającego. Integracja z Istniejącym środowiskiem IT. Wdrożenie VPN – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN.
Przedmiot zamówienia:	Usługa wdrożenia oraz dostosowania serwera, urządzeń sieciowych i oprogramowania zgodnie z wymogami KRI							
Ilość:	1 sztuka							
Wdrożenie urządzenia UTM oraz integracja z środowiskiem IT.	Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do aktualnych wersji oprogramowania. Wydzielenie podsieci VLAN w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgodnie z wymaganiami Zamawiającego. Integracja z Istniejącym środowiskiem IT. Wdrożenie VPN – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN.							

			<p>Wdrożenie wydzielonej, galwanicznej sieci zarządzającej systemami IT.</p> <p>Wdrożenie wykonywane na miejscu.</p> <p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.</p> <p>Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"><li>• Polską Normą PN-ISO/IEC 27002,</li><li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li></ul> <p>Prace zostaną zakończone protokołem.</p>
		Wdrożenie Serwera wraz z kontrolerem zdalnego zarządzania	<p>Fizyczny montaż serwera w siedzibie Zamawiającego. Podłączanie do sieci elektrycznej w tym urządzeń dystrybucji zasilania. Konfiguracja z systemami dystrybucji zasilania Zamawiającego. Montaż serwera z przewodnikami musi zostać wykonany w sposób umożliwiający wysunięcie w czasie pracy. Wszystkie elementy instalacyjne w tym kable sieciowe, kable elektryczne, adaptory zasilania, itp. zapewnia Wykonawca w cenie usługi.</p> <p>Wdrożenie zintegrowanego modułu zdalnego zarządzania serwerem.</p> <p>Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego.</p> <p>Aktualizacja do najnowszej wersji oprogramowania.</p> <p>Zapewnienie konfiguracji wszystkich parametrów w tym macierzy dyskowych zgodnie z wymogami prawa i wytycznymi Zamawiającego.</p> <p>Podłączenie do podsieci zgodnie z wymaganiami Zamawiającego. Integracja z istniejącym środowiskiem IT.</p> <p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.</p> <p>Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"><li>• Polską Normą PN-ISO/IEC 27002,</li><li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li></ul> <p>Prace zostaną zakończone protokołem.</p>
		Wdrożenie Hypevisor	<p>Fizyczna i techniczna Instalacja oprogramowania w siedzibie Zamawiającego wraz z pełną konfiguracją opisaną powyżej. Migracja starego środowiska na nowy Hypervisor. Migracja musi odbyć się z rozbiciem na poszczególne serwery wirtualne zgodnie ze wskazaniami Zamawiającego. Proces przejścia ze starego serwera na nowy serwer trzeba wykonać poza godzinami pracy instytucji, w celu zachowania ciągłości pracy Zamawiającego.</p> <p>Wdrożenie wydzielonej, galwanicznej sieci wirtualnej zarządzającej systemami IT, do wykonywania kopii serwera wirtualnego.</p> <p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania</p>

			<p>naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"><li>• Polską Normą PN-ISO/IEC 27002,</li><li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li></ul> <p>Prace zostaną zakończone protokołem.</p>
		Wdrożenie systemu kopii bezpieczeństwa maszyn wirtualnych	<p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"><li>• Polską Normą PN-ISO/IEC 27002,</li><li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li></ul> <p>Prace zostaną zakończone protokołem.</p>
		Wdrożenie usługi katalogowej Active Directory	<p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"><li>• Polską Normą PN-ISO/IEC 27002,</li><li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li></ul> <p>Instalacja maszyn wirtualnych, systemów operacyjnych i przygotowanie serwerów w tym kontrolerów domeny na potrzeby pracy w Domenie Systemu Windows.</p> <p>Migracja istniejącego środowiska IT Zamawiającego. W przypadku braku możliwości migracji istniejących rozwiązań, wdrożenie od podstaw nowej domeny wraz z przeniesieniem zasobów.</p> <p>Wdrożenie polityk GPO dostosowujących środowisko do wyżej wymienionych wymogów prawa i Zamawiającego - takich jak polityki synchronizacji czasu, dokumentów, haseł, blokowania, dostępu do zasobów, etc.</p> <p>Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencji), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego.</p> <p>Aktualizacja do najnowszych wersji oprogramowania.</p> <p>Wdrożenie usługi File Server, utworzenie, przeniesienie, przypisanie uprawnień i zabezpieczenie zasobów zgodnie z zaleceniami Zamawiającego. (np. dyski wspólne z podziałem uprawnień).</p> <p>Wdrożenie usługi Print Server, wraz z konfiguracją i zabezpieczeniami.</p> <p>Wdrożenie i zabezpieczenie usługi DNS.</p> <p>Przygotowanie maszyn wirtualnych na potrzeby baz danych, podłączenie do domeny oraz ich zabezpieczenie.</p> <p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych, Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail i numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p>



		<p>Udzielenie zdalnego wsparcia dla pracowników IT Zamawiającego, nie będącego następstwem błędów i awarii w liczbie 30 godzin.</p> <p>Prace zostaną zakończone protokołem.</p>
		<p>Instalacja potrzebnych maszyn wirtualnych, systemów operacyjnych i odpowiednie przygotowanie serwera do systemu antywirusowego.</p> <p>Wdrożenie polis GPO umożliwiających dystrybucję spreparowanego agenta w sieci zamawiającego.</p> <p>Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego.</p> <p>Aktualizacja do najnowszej wersji oprogramowania.</p> <p>Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie.</p> <p>Przez 12 miesięcy od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.</p> <p>Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego.</p> <p>Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:</p> <ul style="list-style-type: none"> <li>• Polską Normą PN-ISO/IEC 27002,</li> <li>• Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.</li> </ul> <p>Prace zostaną zakończone protokołem.</p>
		<ul style="list-style-type: none"> <li>• Szkolenie dla działu IT - Migracja komputerów i danych użytkowników do usługi katalogowej Active Directory</li> <li>• Szkolenie dla działu IT – moduł zdalnego zarządzania serwerem</li> <li>• Szkolenie dla działu IT – zarządzanie funkcją hypervisor</li> <li>• Szkolenie dla działu IT – zarządzanie oprogramowaniem do tworzenia kopii zapasowej</li> <li>• Szkolenie dla działu IT – Domena Systemu Windows – zarządzanie (na poziomie MS 55371)</li> </ul> <p>Wszystkie szkolenia wykonane w siedzibie zamawiającego. Szkolenia należy wykonać z uwzględnieniem konfiguracji zastosowanych w systemach IT Zamawiającego. Osoby prowadzące szkolenia muszą posiadać udokumentowaną wiedzę. Szkolenia zakończone protokołem.</p> <p>Wykonawca zapewni nieodpłatne wsparcie w wyżej wymienionym zakresie przez okres 24 miesięcy od zakończenia szkolenia w liczbie 30 godzin. Wsparcie zostanie udzielone w terminie 48 godzin od chwili zgłoszenia.</p> <p>Wykonawca udostępni do kontaktu adres e-mail i numer telefonu. Czas jest liczony od wysłania e-mail przez Zamawiającego.</p> <p>Prace zostaną zakończone protokołem.</p>
17.	Montaż i wdrożenie serwera wraz z układem zarządzającym	Poz. 16
18.	wdrożenie systemu	Poz. 16

	operacyjnego wirtualizacji	
19.	wdrożenie systemów kopii bezpieczeństwa maszyn wirtualnych	Poz. 16
20.	wdrożenie usług katalogowych	Poz. 16
21.	wdrożenie systemu antywirusowego wraz z konsolą zarządzającą	Poz. 16
22.	wdrożenie systemu do zarządzania UPS poprzez sieć	Poz. 16
23.	konfiguracja urządzeń sieciowych w jednostkach podległych, tj. 1 w GOPS, 1 w CUW, 1 w GZGKiM	Poz. 16
24.	wdrożenie usług katalogowych w jednostkach podległych, tj. 1 w GOPS, 1 w CUW, 1 w GZGKiM	Poz. 16
25.	wdrożenie systemu antywirusowego w jednostkach podległych wraz	Poz. 16

	z konsolą zarządzającą, tj. 1 w GOPS, 1 w CUW, 1 w GZGKiM		
26.	serwer plików NAS na 12 dysków wraz z szynami rack	Przedmiot zamówienia:	Zakup serwera plików NAS na 12 dysków wraz z szynami rack
		Ilość:	1 sztuka
		Okres gwarancji producenta min.:	36 miesięcy
		Typ	Sieciowy serwer plików NAS
		Procesor	4-rdzeniowy/8-wątkowy procesor klasy x86, min. 2,2 GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 4557 na dzień 27.10.2025 w teście PassMark dostępnym na stronie internetowej: <a href="https://www.cpubenchmark.net/">https://www.cpubenchmark.net/</a>
		Pamięć RAM	Min. 8 GB DDR4 RAM Możliwość instalacji do 64 GB RAM
		Pamięć flash	Min. 5GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
		Obudowa	<ul style="list-style-type: none"><li>• rack</li><li>• Ilość wnęk na dyski 3.5 cala: minimum 12 szt.</li><li>• Wymiana każdego napędu bez wyłączania serwera (hot-swap): tak</li><li>• Kompatybilność:<ul style="list-style-type: none"><li>◦ 3,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA</li></ul></li><li>• Wysokość obudowa rack: minimum 2U</li><li>• Szyny do szafy rack w zestawie</li></ul>
		Zasilacz	Redundantny, o mocy pojedynczego zasilacza min. 300W, 100–240 V
		Interfejsy sieciowe	<ul style="list-style-type: none"><li>• interfejsy pracujące w technologii 2,5Gbe RJ45 : minimum 2 szt.</li></ul>
		Porty USB oraz gniazda rozszerzeń:	<ul style="list-style-type: none"><li>• Minimum: 2x USB typu C, 1x USB typu A</li><li>• Gniazdo PCIe Gen 3 x4 – minimum 2</li></ul>
		Certyfikaty	Producent serwera NAS musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO 14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego.
		Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej.
27.	serwer plików NAS na 4 dyski	Przedmiot zamówienia:	Zakup serwera plików NAS na 4 dyski
		Ilość:	1 sztuka

		<b>Okres gwarancji producenta min.:</b>	36 miesięcy
		Typ	Sieciowy serwer plików NAS
		Procesor	4-rdzeniowy/8-wątkowy procesor klasy x86, min. 2,2 GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 4557 na dzień 27.10.2025 w teście PassMark dostępnym na stronie internetowej: <a href="https://www.cpubenchmark.net/">https://www.cpubenchmark.net/</a>
		Pamięć RAM	Min. 8 GB DDR4 RAM  Możliwość instalacji do 64 GB RAM
		Pamięć flash	Min. 5GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
		Obudowa	<ul style="list-style-type: none"><li>• Tower / desktop</li><li>• Ilość wnęk na dyski 3.5 cala: minimum 4 szt.</li><li>• Wymiana każdego napędu bez wyłączania serwera (hot-swap): tak</li><li>• Kompatybilność:<ul style="list-style-type: none"><li>◦ 3,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA</li></ul></li><li>• Wysokość obudowa rack: minimum 2U</li></ul>
		Zasilacz	o mocy min. 250W, 100–240 V
		Interfejsy sieciowe	<ul style="list-style-type: none"><li>• interfejsy pracujące w technologii 2,5Gbe RJ45 : minimum 2 szt.</li></ul>
		Porty USB oraz gniazda rozszerzeń:	<ul style="list-style-type: none"><li>• Minimum: 1x USB typu C, 3x USB typu A</li><li>• Gniazdo PCIe Gen 3 x4 – minimum 2</li></ul>
		Certyfikaty	Producent serwera NAS musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO 14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego.
		Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej.
28.	dyski twarde 10TB do serwerów NAS z gwarancją zachowania dysku	<b>Przedmiot zamówienia:</b>	Dyski do serwerów NAS dostarczanych przez wykonawcę
		<b>Ilość:</b>	16 sztuk
		Opis	<ul style="list-style-type: none"><li>• Ilość dysków: 16 szt.</li><li>• Interfejs dysku: SATA3 (6 Gbit/s)</li><li>• Pojemność pojedynczego dysku: minimum 10TB</li><li>• Klasa dysku: Minimum NAS, przeznaczony do pracy ciągłej</li></ul> <p>Dyski muszą znajdować się na oficjalnej liście kompatybilności na stronie producentów serwerów NAS dostarczanych przez Wykonawcę.</p>
29.	switch klasy enterprise z licencjami na 1 rok, 24 portów	<b>Przedmiot zamówienia:</b>	Switch POE z licencjami na 1 rok
		<b>Ilość:</b>	1 sztuka

POE dla jednej GOPS	Okres gwarancji producenta min.:	12 miesięcy
	Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
	Parametry fizyczne platformy	<ul style="list-style-type: none"><li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li><li>Zasilanie AC 230V.</li></ul>
	Interfejsy sieciowe	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ul style="list-style-type: none"><li>24 porty GE RJ-45, w tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af/at.</li><li>4 porty 10 GE SFP+.</li></ul>
	Zarządzanie	<ul style="list-style-type: none"><li>Wbudowany port konsoli szeregowej do pełnego zarządzania.</li><li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li><li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li><li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li><li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li><li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li><li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li><li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li><li>Automatycznie wykonywane rewizje konfiguracji.</li></ul>
	Wymagane funkcje	<ul style="list-style-type: none"><li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>Obsługa Jumbo Frames.</li><li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>Agregacja portów zgodna ze standardem 802.3ad.</li><li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>Port-mirroring.</li><li>Uwierzytelnianie 802.1x na poziomie portu.</li><li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li><li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li><li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li><li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li></ul>

		<p>Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC</p>	<p>4. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"><li>• Centralne zarządzanie konfiguracją urządzenia</li><li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li><li>• Centralne zarządzanie sieciami VLAN.</li><li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li><li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li><li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li><li>• Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.</li><li>• Automatyczna detekcja i rekomendacje konfiguracji.</li><li>• Przesyłanie logów na zewnętrzny serwer syslog.</li><li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li><li>• Obsługa białych i czarnych list adresów MAC.</li><li>• Wykrywanie aplikacji komunikujących się w sieci.</li></ul> <p>5. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>6. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.</p>
		<p>Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa</p>	<ul style="list-style-type: none"><li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym</li><li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li></ul>
		<p>Gwarancja oraz wsparcie</p>	<p>System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.</p>
30.	switch klasy enterprise z licencjami na 2 lata - 24 porty, dla jednostek CUW oraz GZGKiM	Poz. 13	
31.	bezprzewodowe punkty dostępowe klasy enterprise z licencjami na dwa lata dla jednostki - GOPS	Poz. 4	
32.	szkolenia	<p>Przedmiot zamówienia:</p>	<p>Szkolenia online z zakresu cyberbezpieczeństwa</p>

		Ilość:	1 sztuka
		Ilość użytkowników:	30 użytkowników
		Okres gwarancji producenta:	6 m-cy
		Opis	Przedmiotem zamówienia jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy.
		Usługa musi zawierać:	<div><div><div>1.</div><div><div>Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.</div><div><div>a.</div><div>Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:<div><div>i.</div><div>Podstawy bezpiecznego internetu</div></div><div><div>ii.</div><div>Bezpieczeństwo poczty</div></div><div><div>iii.</div><div>Załączniki w poczcie elektronicznej</div></div><div><div>iv.</div><div>Phishing</div></div><div><div>v.</div><div>Spyware/malware</div></div><div><div>vi.</div><div>Bezpieczeństwo danych osobowych RODO/GDRP</div></div><div><div>vii.</div><div>Bezpieczne hasła</div></div><div><div>viii.</div><div>Menedżery haseł</div></div><div><div>ix.</div><div>Bezpieczeństwo urządzeń mobilnych</div></div><div><div>x.</div><div>Uwierzytelnianie wieloskładnikowe (MFA)</div></div><div><div>xi.</div><div>Bezpieczna praca zdalna</div></div><div><div>xii.</div><div>Bezpieczna praca w biurze</div></div><div><div>xiii.</div><div>Sieci społeczne</div></div><div><div>xiv.</div><div>Socjotechnika stosowana</div></div><div><div>xv.</div><div>Zakupy w internecie</div></div></div></div><div><div>b.</div><div>Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.</div></div><div><div>c.</div><div>Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 7 godzin.</div></div></div><div><div>2.</div><div><div>Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail</div><div><div>a.</div><div>z linkiem prowadzącym do stronnym internetowej,</div></div><div><div>b.</div><div>z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,</div></div><div><div>c.</div><div>z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,</div></div></div></div></div></div>

			<div>d. z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.</div> <div>e. W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.</div> <div>3. dedykowaną platformę dostarczającą raporty obejmujące minimum:<div>a. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,</div><div>b. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.</div></div> <div>W ramach świadczonej usługi usługodawca musi:<div><div>• przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,</div><div>• zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,</div><div>• zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,</div><div>• dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,</div><div>• wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).</div></div></div> <td></td> <td><div>Wymagania dodatkowe</div><div>Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.</div><div>Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</div></td>		<div>Wymagania dodatkowe</div> <div>Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.</div> <div>Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</div>
33.	szkolenia w 2 jednostkach podległych, tj. w CUW oraz GZGKiM	<div>Przedmiot zamówienia:</div> <div>Ilość:</div> <div>Ilość użytkowników:</div> <div>Okres gwarancji producenta:</div> <div>Opis</div> <div>Usługa musi zawierać:</div>	<div>Szkolenia online z zakresu cyberbezpieczeństwa</div> <div>2 sztuki</div> <div>10 użytkowników</div> <div>6 m-cy</div> <div>Przedmiotem zamówienia jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy.</div> <div>4. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.<div>a. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:<div>i. Podstawy bezpiecznego internetu</div><div>ii. Bezpieczeństwo poczty</div><div>iii. Załączniki w poczcie elektronicznej</div><div>iv. Phishing</div></div></div>		



			<div><div><div><div><div>v.    Spyware/malware</div><div>vi.    Bezpieczeństwo danych osobowych RODO/GDRP</div><div>vii.    Bezpieczne hasła</div><div>viii.    Menedżery haseł</div><div>ix.    Bezpieczeństwo urządzeń mobilnych</div><div>x.    Uwierzytelnianie wieloskładnikowe (MFA)</div><div>xi.    Bezpieczna praca zdalna</div><div>xii.    Bezpieczna praca w biurze</div><div>xiii.    Sieci społeczne</div><div>xiv.    Socjotechnika stosowana</div><div>xv.    Zakupy w internecie</div></div></div><div><div>b.    Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.</div><div>c.    łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 7 godzin.</div></div><div><div>5.    Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail</div><div><div>a.    z linkiem prowadzącym do stronnym internetowej,</div><div>b.    z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,</div><div>c.    z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,</div><div>d.    z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.</div><div>e.    W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.</div></div></div><div><div>6.    dedykowaną platformę dostarczającą raporty obejmujące minimum:</div><div><div>a.    status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,</div><div>b.    status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.</div></div></div><div><div>W ramach świadczonej usługi usługodawca musi:</div><div><div><div>•    przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,</div><div>•    zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,</div><div>•    zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,</div><div>•    dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,</div></div></div></div></div></div>
--	--	--	--

			<ul style="list-style-type: none"><li>wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).</li></ul>
		Wymagania dodatkowe	<p>Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.</p> <p>Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</p>
34.	szkolenie w jednostce podległej - GOPS	Przedmiot zamówienia:	Szkolenia online z zakresu cyberbezpieczeństwa
		Ilość:	1 sztuka
		Ilość użytkowników:	20 użytkowników
		Okres gwarancji producenta:	6 m-cy
		Opis	Przedmiotem zamówienia jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy.
		Usługa musi zawierać:	<p>7. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.</p> <p>a. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:</p> <ul style="list-style-type: none"><li>i. Podstawy bezpiecznego internetu</li><li>ii. Bezpieczeństwo poczty</li><li>iii. Załączniki w poczcie elektronicznej</li><li>iv. Phishing</li><li>v. Spyware/malware</li><li>vi. Bezpieczeństwo danych osobowych RODO/GDRP</li><li>vii. Bezpieczne hasła</li><li>viii. Menedżery haseł</li><li>ix. Bezpieczeństwo urządzeń mobilnych</li><li>x. Uwierzytelnianie wieloskładnikowe (MFA)</li><li>xi. Bezpieczna praca zdalna</li><li>xii. Bezpieczna praca w biurze</li><li>xiii. Sieci społeczne</li><li>xiv. Socjotechnika stosowana</li><li>xv. Zakupy w internecie</li></ul> <p>b. Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.</p>

			<p>c. łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 7 godzin.</p> <p>8. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail</p> <p>a. z linkiem prowadzącym do stronnym internetowej,</p> <p>b. z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,</p> <p>c. z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,</p> <p>d. z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.</p> <p>e. W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.</p> <p>9. dedykowaną platformę dostarczającą raporty obejmujące minimum:</p> <p>a. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,</p> <p>b. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto stworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.</p> <p>W ramach świadczonej usługi usługodawca musi:</p> <ul style="list-style-type: none"> <li>przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,</li> <li>zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,</li> <li>zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,</li> <li>dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,</li> <li>wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).</li> </ul>
		Wymagania dodatkowe	<p>Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.</p> <p>Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</p>
35.	szkolenia IT	Poz. 16	