



SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

w ramach Projektu „Cyberbezpieczny Powiat Nidzicki” dofinansowanego ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd” realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Główny kod CPV:

32420000-3 - Urządzenia sieciowe

48421000-5 - Pakiety oprogramowania do zarządzania urządzeniami



SPIS TREŚCI

1. [CPNU] Wymagania techniczne w zakresie dostawy, instalacji i konfiguracji urządzenia UTM	3
2. [CPNM] Wymagania techniczne w zakresie oprogramowania do monitorowania infrastruktury informatycznej SPN	10

**1. [CPNU] WYMAGANIA TECHNICZNE W ZAKRESIE DOSTAWY, INSTALACJI I KONFIGURACJI URZĄDZENIA UTM**

W ramach tego podzadania ma być wykonana dostawa, instalacja i konfiguracja 2 szt. routerów brzegowych (UTM) pracujących w trybie wysokodostępного klastra. Routery mają zabezpieczać łącze internetowe w celu zapewnienia redundantnego urządzenia do kontroli ruchu sieciowego i blokowania nieautoryzowanego dostępu do systemów i usług sieciowych.

Lp.	ID	Nazwa wymagania	Wymagalność
1.1.	CPNU_001	Typ obudowy: Wysokość pojedynczego urządzenia maksymalnie 1U. Dołączone 2 szt. półek do zamontowania obydwu urządzeń w szafie rack 19".	MUSI BYĆ
1.2.	CPNU_002	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.	MUSI BYĆ
1.3.	CPNU_003	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.	MUSI BYĆ
1.4.	CPNU_004	Dla wszystkich funkcji systemu wymagane jest dostarczenie dokumentu potwierdzonego przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.	MUSI BYĆ
1.5.	CPNU_005	System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.	MUSI BYĆ
1.6.	CPNU_006	System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.	MUSI BYĆ
1.7.	CPNU_007	Istnieje możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	MUSI BYĆ
1.8.	CPNU_008	System wspiera protokoły IPv4 oraz IPv6 w zakresie: a) Firewall. b) Ochrony w warstwie aplikacji. c) Protokołów routingu dynamicznego.	MUSI BYĆ
1.9.	CPNU_009	Wymagania techniczne w zakresie redundancji, monitoringu i wykrywania awarii: a) System ma pracować w postaci redundantnego klastra. b) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. c) Możliwość monitorowania i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. d) Możliwość monitorowania stanu realizowanych połączeń VPN. e) Możliwość agregacji linków statyczną oraz w oparciu o protokół LACP. f) Możliwość tworzenia interfejsów redundantnych.	MUSI BYĆ
1.10.	CPNU_010	Wymagania techniczne w zakresie interfejsów, dysku i zasilania: a) System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: - 8 portami Gigabit Ethernet RJ-45. - 2 gniazdami SFP+ 10Gbps lub 10 Gigabit Ethernet RJ-45. b) System Firewall posiada wbudowany port konsoli szeregową oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.11.	CPNU_011	Wymagania techniczne w zakresie parametrów wydajnościowych: a) Obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 124 tys. nowych połączeń na sekundę. b) Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. c) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6,7 Gbps.	MUSI BYĆ
1.12.	CPNU_012	Wymagania techniczne w zakresie funkcji systemu bezpieczeństwa: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. b) Kontrola Aplikacji. c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. d) Ochrona przed malware. e) Ochrona przed atakami - Intrusion Prevention System. f) Kontrola stron WWW. g) Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3. h) Zarządzanie pasmem (QoS, Traffic shaping). i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). j) 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. k) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. l) Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. m) 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).	MUSI BYĆ
1.13.	CPNU_013	Wymagania techniczne w zakresie polityk firewall: a) Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. b) System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: - Translację jeden do jeden oraz jeden do wielu. - Dedykowany ALG (Application Level Gateway) dla protokołu SIP. c) W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. d) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. e) Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. f) Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. g) Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. - Amazon Web Services (AWS). - Microsoft Azure. - Cisco ACI. - Google Cloud Platform (GCP). - OpenStack. - VMware NSX. - Kubernetes.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia

Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.14.	CPNU_014	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: a) Wsparcie dla IKE v1 oraz v2. b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) Obsługa protokołu Diffie-Hellman grup 19, 20. d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. l) Mechanizm „Split tunneling” dla połączeń Client-to-Site.	MUSI BYĆ
1.15.	CPNU_015	System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 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. b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 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.	MUSI BYĆ
1.16.	CPNU_016	Wymagania techniczne w zakresie routingu i obsługi łączy WAN: a) Obsługa routingu statycznego. b) Obsługa Policy Based Routing (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). c) Obsługa protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. e) Obsługa ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu. f) Obsługa BFD (Bidirectional Forwarding Detection). g) Obsługa monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	MUSI BYĆ
1.17.	CPNU_017	Wymagania techniczne w zakresie funkcji SD-WAN: a) System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. b) SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	MUSI BYĆ
1.18.	CPNU_018	Wymagania techniczne w zakresie zarządzania pasmem: a) System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. b) System daje możliwość określania pasma dla poszczególnych aplikacji. c) System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. d) System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.19.	CPNU_019	<p>Wymagania techniczne w zakresie ochrony przed malware:</p> <p>a) Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>b) Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>c) 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.</p> <p>d) System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>e) System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>f) Baza sygnatur jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>g) 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.</p> <p>h) System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>i) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.</p> <p>j) Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>	MUSI BYĆ
1.20.	CPNU_020	<p>Wymagania techniczne w zakresie ochrony przed atakami:</p> <p>a) Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>b) System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>c) Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>d) System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>e) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>f) Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>g) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>h) Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>	MUSI BYĆ
1.21.	CPNU_021	<p>Wymagania techniczne w zakresie kontroli aplikacji:</p> <p>a) Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>b) Baza Kontroli Aplikacji jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>c) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>d) Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>e) Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>f) Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>g) 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).</p>	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.22.	CPNU_022	<p>Wymagania techniczne w zakresie kontroli WWW:</p> <p>a) Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii tematyczne.</p> <p>b) 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.</p> <p>c) Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>d) Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>e) Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>f) Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>g) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>h) Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>i) System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>	MUSI BYĆ
1.23.	CPNU_023	<p>Wymagania techniczne w zakresie funkcji uwierzytelniania użytkowników w ramach sesji:</p> <p>a) System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>b) System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>c) 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.</p> <p>d) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>	MUSI BYĆ
1.24.	CPNU_024	<p>Wymagania techniczne w zakresie zarządzania:</p> <p>a) Elementy systemu bezpieczeństwa mają możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>b) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>c) Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>d) System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>e) Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>f) Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>g) Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>h) Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>i) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.25.	CPNU_025	<p>Wymagania techniczne w zakresie logowania:</p> <p>a) 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.</p> <p>b) W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>c) Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>d) Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>e) System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>f) Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>	MUSI BYĆ
1.26.	CPNU_026	<p>Dostarczone subskrypcje na okres do 30 czerwca 2026. Subskrypcja ma upoważniać Zamawiającego do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:</p> <p>a) Ochrona przed atakami - Intrusion Prevention System</p> <p>b) Ochrona przed malware</p> <p>c) Kontrola aplikacji</p> <p>d) Kontrola stron WWW</p> <p>e) Kontrola zawartości poczty</p>	MUSI BYĆ
1.27.	CPNU_027	<p>Gwarancja 24 miesiące. UTM jest objęty serwisem gwarancyjnym producenta realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>	MUSI BYĆ
1.28.	CPNU_028	<p>System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.</p>	MUSI BYĆ
1.29.	CPNU_029	<p>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>a) Wsparcie telefoniczne zespołu certyfikowanych inżynierów.</p> <p>b) Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</p> <p>c) Doradztwo w zakresie konfiguracji.</p> <p>d) Zdalne wsparcie techniczne.</p> <p>e) Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</p> <p>f) Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).</p> <p>g) Przygotowanie urządzenia do zdalnej konfiguracji.</p> <p>h) Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</p> <p>i) Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</p> <p>j) Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</p> <p>k) Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</p>	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
1.30.	CPNU_030	<p>Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</p> <p>Wymagania powinny być potwierdzone dokumentami:</p> <p>a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</p> <p>b) Certyfikat ISO 9001 podmiotu serwisującego.</p>	MUSI BYĆ
1.31.	CPNU_031	<p>Opisy do wymagań ogólnych:</p> <p>a) Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>b) Wymaga się, aby Wykonawca uzyskał i przedstawił Zamawiającemu dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.</p>	MUSI BYĆ



2. [CPNM] WYMAGANIA TECHNICZNE W ZAKRESIE OPROGRAMOWANIA DO MONITOROWANIA INFRASTRUKTURY INFORMATYCZNEJ SPN

W ramach tego podzadania ma zostać dostarczona licencja na korzystanie z oprogramowania do monitorowania infrastruktury informatycznej Starostwa Powiatowego w Nidzicy wraz z usługami serwisowymi.

Obecnie w SPN jest eksploatowane oprogramowanie firm Axence Sp. z o. o.: Axence nVision

Lp.	ID	Nazwa wymagania	Wymagalność
2.1.	CPNM_001	Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem, a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.	MUSI BYĆ
2.2.	CPNM_002	Moduły oprogramowania umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwany użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source dzięki czemu nie jest objęty limitem ilości danych. Baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.	MUSI BYĆ
2.3.	CPNM_003	Oprogramowanie musi umożliwiać instalację agenta w systemie Windows wraz z ochroną przed usunięciem agenta.	MUSI BYĆ
2.4.	CPNM_004	Oprogramowanie umożliwia ustawienie alarmów typu zdarzenie-akcja.	MUSI BYĆ
2.5.	CPNM_005	Oprogramowanie umożliwia ustawienie powiadomień (pulpitowe, e-mailowe, SMS-owe) oraz akcji korekcyjnych (uruchomienie programu, restart komputera itp.).	MUSI BYĆ
2.6.	CPNM_006	Oprogramowanie umożliwia ustawienie powiadomień o alarmach wysyłane za pośrednictwem komunikatorów MS Teams i Slack.	MUSI BYĆ
2.7.	CPNM_007	Oprogramowanie umożliwia ustawienie powiadomień o alarmach za pośrednictwem serwisu smsapi.pl.	MUSI BYĆ
2.8.	CPNM_008	Oprogramowanie umożliwia obsługę OAuth 2.0 dla wysyłki wiadomości e-mail i SMS.	MUSI BYĆ
2.9.	CPNM_009	Oprogramowanie umożliwia zarządzanie hierarchią użytkowników (w tym import z AD).	MUSI BYĆ
2.10.	CPNM_010	Oprogramowanie umożliwia ustawienie raportów dla użytkowników, urządzeń, oddziałów, map sieci lub całego atlasu.	MUSI BYĆ
2.11.	CPNM_011	Oprogramowanie umożliwia jednoczesną pracę wielu administratorów, dziennik dostępu administratorów.	MUSI BYĆ
2.12.	CPNM_012	Oprogramowanie umożliwia zarządzanie uprawnieniami wielu administratorów.	MUSI BYĆ
2.13.	CPNM_013	Oprogramowanie umożliwia zarządzanie grupami (tworzenie, przypisywanie użytkowników).	MUSI BYĆ
2.14.	CPNM_014	Oprogramowanie umożliwia menu kontekstowe z możliwością definiowania własnych narzędzi.	MUSI BYĆ
2.15.	CPNM_015	Oprogramowanie umożliwia ustawienie dziennika dostępu administratorów: wysyłanie zdarzeń do zewnętrznego kolektora Syslog.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
2.16.	CPNM_016	Oprogramowanie posiada globalną wyszukiwarkę w konsoli, globalne wyszukiwanie obiektów np.: urządzeń, użytkowników, zasobów oraz elementów interfejsu programu (np. opcji).	MUSI BYĆ
2.17.	CPNM_017	Oprogramowanie umożliwia logowanie w konsoli deinstalacji Agenta.	MUSI BYĆ
2.18.	CPNM_018	Oprogramowanie umożliwia ustawienie uwierzytelniania wieloskładnikowego (Multifactor Authentication/MFA).	MUSI BYĆ
2.19.	CPNM_019	Oprogramowanie posiada zwiększone wymagania dla haseł użytkowników.	MUSI BYĆ
2.20.	CPNM_020	Oprogramowanie umożliwia szyfrowaną synchronizację z Active Directory z wykorzystaniem LDAPS (Secure LDAP).	MUSI BYĆ
2.21.	CPNM_021	Oprogramowanie posiada następujące funkcjonalności konsoli administracyjnej: a) prezentowanie wybranych danych w przeglądarce internetowej za pomocą widgetów b) responsywne widgety, zarządzanie rozmiarem siatki widgetów c) automatyczne odświeżanie dashboardów d) wyświetlanie dashboardów w trybie jasnym i ciemnym e) udostępnianie dashboardów w trybie tylko do odczytu f) zarządzanie uprawnieniami administratorów do funkcjonalności konsoli administracyjnej g) widgety dla modułu sieciowego: liczniki wydajności, alarmy oraz odpowiedzi serwisów TCP/IP, mapa sieci h) widgety dla modułu inwentaryzacji: zmiany w konfiguracji sprzętowej urządzeń z agentami, zmiany w liście zainstalowanego oprogramowania, alarmy dla zasobów i) widgety dla modułu użytkowników: statystyki z obszaru wydruków, statystyki użycia aplikacji, użycie łącza, aktywność WWW, rejestr naruszeń blokad j) widgety dla modułu wsparcia użytkowników: statystyki z obsługi zgłoszeń, lista najnowszych nierozwiązanych zgłoszeń, lista najstarszych nierozwiązanych zgłoszeń, ostatnie 10 zgłoszeń ze złamaną metryką SLA, 10 najbliższych metryk SLA k) widgety dla modułu ochrony danych: ostatnio podłączone nośniki zewnętrzne, ostatnie operacje na plikach, BitLocker, antywirus, firewall	MUSI BYĆ
2.22.	CPNM_022	Oprogramowanie posiada następujące funkcjonalności modułu sieciowego: a) Możliwość skanowania sieci, wykrywania urządzeń i serwisów TCP/IP. b) Interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne. c) Serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL). d) Liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy. e) Działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń. f) Liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne). g) Kompilator plików MIB. h) Obsługa pułapek SNMP. i) Routery i switchy: mapowanie portów; informacja, do którego przełącznika jest podłączone urządzenie. k) Obsługa komunikatów Syslog. l) Możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca). m) Monitorowanie i zarządzanie maszynami wirtualnymi VMware.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
2.23.	CPNM_023	<p>Oprogramowanie posiada następujące funkcjonalności modułu inwentaryzacji:</p> <ul style="list-style-type: none">a) Możliwość zarządzanie wszelkimi zasobami, za które odpowiada dział IT.b) Szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu.c) Widok zasobów, aplikacji, dokumentów, licencji dla poszczególnych użytkowników lub osobny widok według zasobów przypisanych do urządzeń.d) Jednoczesne przypisywanie dokumentu do wielu zasobów.e) Uprawnienia dostępu administratorów do typów zasobów, licencji i dokumentów w ramach oddziałów.f) Masowa edycja atrybutów zasobów, np. statusu.g) Rozbudowany system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji.h) Rozliczanie dowolnego typu licencji, w tym modelowanie licencji chmurowych.i) Rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji.j) Audyt inwentaryzacji sprzętu i oprogramowania.k) Wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach.l) Zdalny dostęp do menedżera plików z możliwością usuwania plików użytkownika.m) Informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej.n) Szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej.o) Zarządzanie instalacjami/deinstalacjami oprogramowania przez menedżera pakietów MSI.p) Alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych.q) Aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR, generowanie etykiet w konsoli.r) Możliwość archiwizacji i porównywania audytów.s) Mobilny Asystent Inwentaryzacji dla systemu Android: wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycja zasobów, dodawanie czynności serwisowych, drukowanie etykiet.t) Generator dokumentów na podstawie szablonów.u) Automatyczne numerowanie dodawanych zasobów oraz dokumentów wg zdefiniowanego wzorca numeracji.v) Historia użycia konkretnej licencji oprogramowania.w) Odczyt danych S.M.A.R.T. z dysków NVMe.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
2.24.	CPNM_024	<p>Oprogramowanie posiada następujące funkcjonalności modułu użytkowników:</p> <ul style="list-style-type: none">a) Pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa.b) Blokowanie uruchamianych aplikacji.c) Monitorowanie wiadomości e-mail (nagłówki) – antyphishing.d) Szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy).e) Użytkowane aplikacje (aktywnie i nieaktywnie)f) Odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt).g) Audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków.h) Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu).i) Zrzuty ekranowe (historia pracy użytkownika ekran po ekranie).j) Blokowanie stron WWW.k) Rejestr naruszeń blokad agregujący informacje o próbie dostępu do blokowanych stron WWW, uruchamianiu zakazanych aplikacji oraz pobieraniu plików z niedozwolonymi rozszerzeniami.l) Dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad.m) Możliwość korzystania z zewnętrznych list blokowania stron, w tym z listą ostrzeżeń CERT.PL.n) Zgodność z RODO – przyporządkowanie konfiguracji, uprawnień i dostępu do konkretnego użytkownika niezależnie od urządzenia.o) Informatyka śledcza – szczegółowe wyszczególnienie aktywności oraz metryki użytkownika.p) Blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXEr) Reguły filtrowania stron WWW i blokowania aplikacji: zmiana mechanizmu tworzenia i zarządzania regułami, grupowanie reguł.s) Reguły filtrowania stron WWW i blokowania aplikacji: powielanie reguł między grupami użytkowników.t) Możliwość wykrywania podejrzanych aktywności użytkowników.u) Możliwość użycia maski * w wykluczeniach w integracji ze stosem TCP/IP.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
2.25.	CPNM_025	<p>Oprogramowanie posiada następujące funkcjonalności modułu wsparcia użytkowników:</p> <ul style="list-style-type: none">a) Tworzenie i procesowanie zgłoszeń serwisowych poprzez intuicyjny interfejs webowy lub za pośrednictwem maila.b) Możliwość planowania zastępstw w przydzielaniu zgłoszeń.c) Możliwość wskazania osób, które muszą zaakceptować zgłoszenie.d) Tworzenie ścieżek akceptacji na podstawie kategorii.e) Automatyczna wysyłka powiadomień do osób akceptujących zgłoszenie.f) Kiosk z aplikacjami – możliwość stworzenia listy bezpiecznych aplikacji do samodzielnej instalacji przez użytkownika.g) Obsługa umów o gwarantowanym poziomie świadczenia usług (SLA).h) Automatyczne przypisywanie zgłoszeń do obsługującego na podstawie określonych warunków.i) Wyszukiwarka oraz aktualizacja zgłoszeń w czasie rzeczywistym.j) Możliwość definiowania reguł widoczności zgłoszeń oraz automatyzacje bazujące na warunkach.k) Możliwość ograniczenia tworzenia zgłoszeń i dostępności artykułów w bazie wiedzy przez wybrane grupy użytkowników tylko w określonych kategoriach.l) Rozbudowany system raportów.m) Możliwość przetwarzania zgłoszeń w trybie anonimowym.n) Możliwość dodawania komentarzy i załączników w zgłoszeniach oraz dodawania pól niestandardowych.o) Obsługa wizytówek użytkowników.p) Wewnętrzny komunikator (czat) z możliwością przesyłania plików.r) Możliwość jednoczesnej pracy wielu administratorów z komunikatami.s) Możliwość wysyłania komunikatów do użytkowników/komputerów z opcją obowiązkowego potwierdzenia odczytu.t) Możliwość wyświetlania historii komunikatów w Agencie.u) Możliwość tworzenia szkiców i archiwizacji komunikatów.w) Zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury.x) Równoczesny zdalny dostęp kilku administratorów do jednego Agentu oraz pełna obsługa sesji terminalowych.y) Możliwość wyboru wyświetlanego ekranu w trakcie trwania zdalnego dostępu.z) Obsługa integracji użytkowników z Active Directory.aa) Obsługa zadań dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania); dwukierunkowa wymiana plików.bb) Baza wiedzy z wbudowaną wyszukiwarką i możliwością dodawania multimediów.cc) Zdalny dostęp do menedżera plików z możliwością usuwania plików użytkownika.dd) Zarządzanie kontami lokalnych użytkowników Windows.ee) Dokumenty prawne dot. ochrony sygnalistów.ff) Możliwość dodania opisu kategorii zgłoszenia np. w celu umieszczenia klauzuli RODO.gg) Obsługa dark mode w systemie zgłoszeń i w czacie.hh) Możliwość zdalnej edycji rejestru na komputerach z zainstalowanym Agentem.ii) Możliwość eksportu listy zgłoszeń do pliku.	MUSI BYĆ



Załącznik nr 2. do szacowania - Opis Przedmiotu Zamówienia



Dostawa, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa

Lp.	ID	Nazwa wymagania	Wymagalność
2.26.	CPNM_026	Oprogramowanie posiada następujące funkcjonalności modułu ochrony danych: a) Informacje o urządzeniach podłączonych do danego komputera. b) Lista wszystkich urządzeń podłączonych do komputerów w sieci. c) Audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych. d) Monitorowanie operacji na plikach w katalogach na dysku systemowym. e) Monitorowanie operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez Agenta np. macierze Synology, Qnap itp. f) Zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników. g) Centralna konfiguracja: ustawienie reguł dla całej sieci oraz grup i użytkowników Active Directory. h) Integracja bazy użytkowników i grup z Active Directory. i) Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym oraz na dyskach lokalnych. j) Wykrywanie oprogramowania antywirusowego innego niż Windows Defender. k) Integracja z Windows BitLocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów. l) możliwość zdalnego szyfrowania dysków za pomocą funkcji BitLocker. m) Integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych. n) Obsługa atrybutu „nośnik zaufany”. o) Automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa. p) Możliwość usuwania nieistniejących/ zutilizowanych nośników danych (np. USB). r) Obsługa metryk użytkowników prezentujących aktualne ustawienia dla danego pracownika. s) Integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania.	MUSI BYĆ
2.27.	CPNM_027	Wymagana licencja na 60 urządzeń.	MUSI BYĆ
2.28.	CPNM_028	Dostarczona subskrypcja na okres do 30 czerwca 2026. Subskrypcja ma upoważniać Zamawiającego do korzystania z aktualizacji oprogramowania.	MUSI BYĆ