

## SPIS TREŚCI

**I. OBSZAR TECHNICZNY**

1. UTM UNIFIED THREAT MANAGMENT: WZMOCNIENIE SUPORTU.....	2
2. UNIFIED THREAT MANAGEMENT: URZĄDZENIE KLASY UTM.....	10
3. SERWER DLA URZĘDU GMINY.....	19
4. SERWER DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	24
5. NETWORK ATTACHED STORAGE NAS: MACIERZ NAS WRAZ Z DYSKAMI DLA URZĘDU GMINY.....	28
6. NETWORK ATTACHED STORAGE NAS: MACIERZ NAS WRAZ Z DYSKAMI DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	30
7. GENERATOR PRĄDU: AGREGAT PRĄDOTWÓRCZY.....	32
8. UPS STANOWISKOWY: UPS DLA URZĘDU GMINY.....	34
9. UPS STANOWISKOWY: UPS DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	36
10. UPS DO SERWERA DLA URZĘDU GMINY.....	37
11. UPS DO SERWERA DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	39
12. ZARZĄDZALNE URZĄDZENIA SIECIOWE Z OBSŁUGĄ VLAN, MACSEC, STANDARDU 802.1X. PRZEŁĄCZNIK ZARZĄDZALNY DLA URZĘDU GMINY.....	40
13. BIBLIOTEKA TAŚMOWA DLA URZĘDU GMINY.....	42
14. OPROGRAMOWANIE ANTYWIRUSOWE Z EDR DLA URZĘDU GMINY.....	44
13. OPROGRAMOWANIE ANTYWIRUSOWE: OPROGRAMOWANIE ANTYWIRUSOWE DLA TELEFONÓW DLA URZĘDU GMINY.....	60
16. OPROGRAMOWANIE ANTYWIRUSOWE: OPROGRAMOWANIE ANTYWIRUSOWE DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	62
17. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH DLA URZĘDU GMINY.....	73
18. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	75
19. OPROGRAMOWANIE SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) DLA URZĘDU GMINY.....	77
20. OPROGRAMOWANIE PRZECIWDZIAŁAJĄCE WYCIEKOWI DANYCH DLP- DATA LEAK PREVENTION DLA URZĘDU GMINY I GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ.....	80
21. OPROGRAMOWANIE DO MONITOROWANIA INFRASTRUKTURY INFORMATYCZNEJ DLA URZĘDU GMINY.....	83
22. USŁUGI INFORMATYCZNE: WDROŻENIE SYSTEMU MONITOROWANIA ŚRODOWISKA SERWEROWEGO.....	85

**II OBSZAR KOMPETENCYJNY**

1. Szkolenie dla Działu IT (Szkolenie dot. UTM).....	87
2. Szkolenie dla Działu IT (Szkolenie Microsoft Active Directory.....	88
3. Szkolenie dla pracowników spoza Działu IT (Cyberbezpieczeństwo).....	90

I. OBSZAR TECHNICZNY

1. UTM Unified Threat Management: wznowienie supportu

Nazwa	Minimalne wymagania dla sprzętu	
Typ	UTM (Unified Threat Management): Wznowienie wsparcia dla posiadanego urządzenia klasy UTM	SPEŁNIA TAK /NIE
Wymagania podstawowe	<p>W ramach dostawy Zamawiający wymaga dostarczenia wznowienia serwisów dla posiadanego obecnie urządzenia klasy UTM Fortigate 40F o numerze seryjnym: FGT40FTK2209DBSK z aktywnym wsparciem producenta do dnia 08.11.2024 na okres minimum 12 miesięcy.</p> <p>Zamawiający wymaga przedłużenia wsparcia producenta licencji w zakresie minimum tj.: Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS &amp; Video Filtering, Antispam Service, and FortiCare Premium)</p> <p>Zamawiający dopuszcza dostarczenie urządzenia klasy UTM równoważnego (tj. wymianę w/w urządzenia klasy UTM) spełniającego poniższe wymagania minimalne.</p> <p>Ponadto, w przypadku dostawy rozwiązania równoważnego Zamawiający wymaga dodatkowo:</p> <ul style="list-style-type: none"><li>- wdrożenia i montażu we wskazanej szafie RACK</li><li>- skonfigurowania dla wszystkich użytkowników</li><li>- przeszkolenia administratorów z dostarczonego rozwiązania, wg ustaleń z Zamawiającym.</li></ul>	SPEŁNIA TAK /NIE
OPIS RÓWNOWAŻNOŚCI – wymagania minimalne:		
Wymagania Ogólne	System bezpieczeństwa musi realizować 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.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>System realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi istnieć możliwość dedykowania co najmniej 7 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 – musi istnieć możliwość łączenia w klastery 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 protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</li></ol>	SPEŁNIA TAK /NIE
Interfejsy, dysk, zasilanie	<ol style="list-style-type: none"><li>1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:<ul style="list-style-type: none"><li>• 5 portów Gigabit Ethernet RJ-45.</li></ul></li><li>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li><li>3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li><li>4. System musi być wyposażony w zasilanie AC.</li></ol>	SPEŁNIA TAK /NIE
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps</p>	
<p><b>Funkcje systemu bezpieczeństwa</b></p>	<p>W ramach systemu ochrony muszą być 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 dwuskładnikowego 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 musi posiadać 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>	<p>SPEŁNIA TAK /NIE</p>
<p><b>Polityki, Firewall</b></p>	<ol style="list-style-type: none"><li>1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li><li>2. System mus realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<ul style="list-style-type: none"><li>• Translację jeden do jeden oraz jeden do wielu.</li><li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li></ul></li></ol>	<p>SPEŁNIA TAK /NIE</p>

Opis przedmiotu zamówienia

	<div><div>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</div><div>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</div><div>5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</div><div>6. Polityka firewall musi umożliwiać ustawienie przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</div></div>	
Połączenia VPN	<div><div>1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:<ul style="list-style-type: none"><li>Wsparcie dla IKE v1 oraz v2.</li><li>Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li><li>Obsługa protokołu Diffie-Hellman grup 19, 20.</li><li>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li><li>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li><li>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li><li>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li><li>Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li><li>Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li><li>Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li><li>Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li><li>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li></ul></div><div>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:<ul style="list-style-type: none"><li>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.</li></ul></div></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><li>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li><li>Producent rozwiązania musi posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klient VPN jest dostępne jako opcja i nie jest wymagane w implementacji.</li></ul>	
Routing i obsługa łącz WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ul style="list-style-type: none"><li>Routing statycznego.</li><li>Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li><li>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</li><li>Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li><li>ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li><li>BFD (Bidirectional Forwarding Detection).</li><li>Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li></ul>	SPEŁNIA TAK /NIE
Funkcję SD-WAN	<ol style="list-style-type: none"><li>System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.</li><li>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).</li></ol>	SPEŁNIA TAK /NIE
Zarządzanie pasmem	<ol style="list-style-type: none"><li>System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li><li>System musi dawać możliwość określania pasma dla poszczególnych aplikacji.</li><li>System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li><li>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</li></ol>	SPEŁNIA TAK /NIE
Ochrona przed malware	<ol style="list-style-type: none"><li>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 21).</li><li>Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li></ol>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<div><div></div><div><div><div>3. System musi umożliwiać 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 musi umożliwiać 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 musi dysponować 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 musi współpracować 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 musi zapewniać 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 laboratoria producenta.</div><div>10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</div></div></div></div>	
Ochrona przed atakami	<div><div></div><div><div><div>1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</div><div>2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.</div><div>3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div><div>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</div><div>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</div><div>6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</div><div>7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</div><div>8. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</div></div></div></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<p>9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>	
Kontrola aplikacji	<p>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>	SPEŁNIA TAK /NIE
Kontrola WWW	<p>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard.</p> <p>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>6. Filtr WWW musi dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p>	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div>8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</div> <div>9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</div>	
Uwierzytelnianie użytkowników w ramach sesji	<div>1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none"><li>Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li><li>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li><li>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li></ul></div> <div>2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</div> <div>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.</div> <div>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</div>	SPEŁNIA TAK /NIE
Zarządzanie	<div>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.</div> <div>2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</div> <div>3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</div> <div>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</div> <div>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</div> <div>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</div> <div>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</div> <div>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</div>	
Logowanie	<div>1. Elementy systemu bezpieczeństwa muszą realizować 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.</div> <div>2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać 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.</div> <div>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</div> <div>4. Możliwość włączenia logowania per reguła w polityce firewall.</div> <div>5. System zapewnia możliwość logowania do serwera SYSLOG.</div> <div>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS</div>	SPEŁNIA TAK /NIE
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.	SPEŁNIA TAK /NIE
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.	SPEŁNIA TAK /NIE
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

2. Unified Threat Management: urządzenie klasy UTM

Nazwa	Minimalne wymagania dla sprzętu
-------	---------------------------------

Opis przedmiotu zamówienia



Typ	UTM (Unified Threat Management: urządzenie klasy UTM)	SPEŁNIA TAK /NIE
Wymagania Ogólne	<p>System bezpieczeństwa musi realizować 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 musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi istnieć możliwość dedykowania co najmniej 7 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>	SPEŁNIA TAK /NIE
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"><li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster 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 łączy sieciowych.</li><li>3. Monitoring stanu realizowanych połączeń VPN.</li><li>4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</li></ol>	SPEŁNIA TAK /NIE
Interfejsy, dysk, zasilanie	<ol style="list-style-type: none"><li>1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:<ul style="list-style-type: none"><li>• 5 portów Gigabit Ethernet RJ-45.</li></ul></li><li>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li></ol>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<div>3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</div> <div>4. System musi być wyposażony w zasilanie AC.</div>	
<div>Parametry wydajnościowe</div>	<div>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</div> <div>Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</div> <div>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</div> <div>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.</div> <div>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.</div> <div>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.</div> <div>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps</div>	<div>SPEŁNIA TAK /NIE</div>
<div>Funkcje systemu bezpieczeństwa</div>	<div>W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</div> <div><div><div>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</div><div>2. Kontrola Aplikacji.</div><div>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</div><div>4. Ochrona przed malware.</div><div>5. Ochrona przed atakami - Intrusion Prevention System.</div><div>6. Kontrola stron WWW.</div><div>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</div><div>8. Zarządzanie pasmem (QoS, Traffic shaping).</div><div>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</div><div>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</div><div>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</div><div>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</div></div></div>	<div>SPEŁNIA TAK /NIE</div>

Opis przedmiotu zamówienia

	13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	
Polityki, Firewall	<div>1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</div> <div>2. System mus realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<ul style="list-style-type: none"><li>Translację jeden do jeden oraz jeden do wielu.</li><li>Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li></ul></div> <div>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</div> <div>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</div> <div>5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</div> <div>6. Polityka firewall musi umożliwiać ustawienie przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</div>	SPEŁNIA TAK /NIE
Połączenia VPN	<div>1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:<ul style="list-style-type: none"><li>Wsparcie dla IKE v1 oraz v2.</li><li>Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li><li>Obsługa protokołu Diffie-Hellman grup 19, 20.</li><li>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li><li>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li><li>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li><li>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li><li>Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li><li>Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li></ul></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<ul style="list-style-type: none"><li>Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li><li>Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li><li>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li></ul> <p>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"><li>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.</li><li>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li><li>Producent rozwiązania musi posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klient VPN jest dostępne jako opcja i nie jest wymagane w implementacji.</li></ul>	
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie musi zapewniać obsługę:</p> <ul style="list-style-type: none"><li>Routingu statycznego.</li><li>Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li><li>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</li><li>Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li><li>ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li><li>BFD (Bidirectional Forwarding Detection).</li><li>Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li></ul>	SPEŁNIA TAK /NIE
Funkcję SD-WAN	<p>1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>	SPEŁNIA TAK /NIE
Zarządzanie pasmem	<p>1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div><div>2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji.</div><div>3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</div><div>4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</div></div>	
Ochrona przed malware	<div><div>1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</div><div>2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</div><div>3. System musi umożliwiać 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 musi umożliwiać 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 musi dysponować 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 musi współpracować 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 musi zapewniać 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 laboratoria producenta.</div><div>10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</div></div>	SPEŁNIA TAK /NIE
Ochrona przed atakami	<div><div>1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</div><div>2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.</div><div>3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div><div></div><div><div><div>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</div><div>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</div><div>6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</div><div>7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</div><div>8. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</div><div>9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</div></div></div></div> <tr><td>Kontrola aplikacji</td><td><div><div></div><div><div><div>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</div><div>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div><div>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</div><div>4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</div><div>5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</div><div>6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</div><div>7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</div></div></div></div><div>SPEŁNIA TAK /NIE</div></td></tr> <tr><td>Kontrola WWW</td><td><div><div></div><div><div><div>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</div><div>2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</div><div>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard.</div></div></div></div><div>SPEŁNIA TAK /NIE</div></td></tr>	Kontrola aplikacji	<div><div></div><div><div><div>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</div><div>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div><div>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</div><div>4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</div><div>5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</div><div>6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</div><div>7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</div></div></div></div> <div>SPEŁNIA TAK /NIE</div>	Kontrola WWW	<div><div></div><div><div><div>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</div><div>2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</div><div>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard.</div></div></div></div> <div>SPEŁNIA TAK /NIE</div>
Kontrola aplikacji	<div><div></div><div><div><div>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</div><div>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</div><div>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</div><div>4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</div><div>5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</div><div>6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</div><div>7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</div></div></div></div> <div>SPEŁNIA TAK /NIE</div>				
Kontrola WWW	<div><div></div><div><div><div>1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</div><div>2. W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</div><div>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: Hazard.</div></div></div></div> <div>SPEŁNIA TAK /NIE</div>				



	<ol style="list-style-type: none"> <li>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</li> <li>Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</li> <li>Filtr WWW musi dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</li> <li>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</li> <li>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</li> <li>System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</li> </ol>	
<b>Uwierzytelnianie użytkowników w ramach sesji</b>	<ol style="list-style-type: none"> <li>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> <li>Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul> </li> <li>System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</li> <li>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>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</li> </ol>	SPEŁNIA TAK /NIE
<b>Zarządzanie</b>	<ol style="list-style-type: none"> <li>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>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</li> <li>Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</li> <li>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</li> </ol>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div><div>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</div><div>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</div><div>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</div><div>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</div><div>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</div></div>	
Logowanie	<div><div>1. Elementy systemu bezpieczeństwa muszą realizować 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.</div><div>2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanim ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</div><div>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</div><div>4. Możliwość włączenia logowania per reguła w polityce firewall.</div><div>5. System zapewnia możliwość logowania do serwera SYSLOG.</div><div>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS</div></div>	SPEŁNIA TAK /NIE
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.	SPEŁNIA TAK /NIE
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.	SPEŁNIA TAK /NIE
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta na okres minimum do 18.04.2026, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	
Ilość	1 szt.	SPEŁNIA TAK /NIE

3. Serwer dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Serwer (serwer do klastra) dla Urzędu Gminy	SPEŁNIA TAK /NIE
Obudowa	Obudowa Rack o wysokości maksymalnej 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz z organizatorem kabli.	SPEŁNIA TAK /NIE
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera	SPEŁNIA TAK /NIE
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	SPEŁNIA TAK /NIE
Procesor	Zainstalowany minimum jeden procesory min. 16-rdzeniowe, min. 2.4GHz, 24MB cache klasy x86 dedykowane do pracy z zaoferowanym serwerem.	SPEŁNIA TAK /NIE
RAM	Minimum 64GB(2x32GB) DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	SPEŁNIA TAK /NIE
Gniazda PCI	Minimum 1x slot PCIe x16 generacji 4	SPEŁNIA TAK /NIE
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT	SPEŁNIA TAK /NIE
Dyski twarde	Dedykowany moduł dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 480GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.	SPEŁNIA TAK /NIE
Kontroler RAID	HBA SAS z portami zewnętrznymi	SPEŁNIA TAK /NIE
Wbudowane porty	Minimum 4 x USB z czego nie mniej niż 1x USB 3.0, minimum 2xVGA z czego jeden na panelu przednim.	SPEŁNIA TAK /NIE
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	SPEŁNIA TAK /NIE
Zasilacze	Redundantne, Hot-Plug minimum 700W każdy	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



Bezpieczeństwo	<ul style="list-style-type: none"><li>• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li><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></ul>	SPEŁNIA TAK /NIE
Diagnostyka	panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.	SPEŁNIA TAK /NIE
Karta zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <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 autentykacje 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></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<ul style="list-style-type: none"><li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li></ul>	
Oprogramowanie do zarządzania	<ul style="list-style-type: none"><li>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li><li>• integracja z Active Directory</li><li>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li><li>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li><li>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li><li>• Szczegółowy opis wykrytych systemów oraz ich komponentów</li><li>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li><li>• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li><li>• Grupowanie urządzeń w oparciu o kryteria użytkownika</li><li>• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li><li>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li><li>• Szybki podgląd stanu środowiska</li><li>• Podsumowanie stanu dla każdego urządzenia</li><li>• Szczegółowy status urządzenia/elementu/komponentu</li><li>• Generowanie alertów przy zmianie stanu urządzenia.</li><li>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li><li>• Integracja z service desk producenta dostarczonej platformy sprzętowej</li><li>• Możliwość przejęcia zdalnego pulpitu</li><li>• Możliwość podmontowania wirtualnego napędu</li><li>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li><li>• Możliwość importu plików MIB</li><li>• Przesyłanie alertów „as-is” do innych konsol firm trzecich</li><li>• Możliwość definiowania ról administratorów</li><li>• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li><li>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li><li>• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<ul style="list-style-type: none"><li>• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li><li>• 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 aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li><li>• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li><li>• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</li><li>• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li><li>• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li><li>• Zdalne uruchamianie diagnostyki serwera.</li><li>• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li><li>• Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li></ul>	
Certyfikaty	<ul style="list-style-type: none"><li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub normami równoważnymi</li><li>• Serwer musi posiadać deklarację CE lub normami równoważnymi</li><li>• Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.</li><li>• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2016, Microsoft Windows 2019.</li></ul>	SPEŁNIA TAK /NIE
Warunki gwarancji	Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta. Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie oświadczenia producenta oferowanego sprzętu.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<p>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).Firma serwisująca musi posiadać ISO 9001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.</p> <p>Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie:</p> <ul style="list-style-type: none"><li>• realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;</li><li>• firma serwisująca posiada autoryzacje producenta oferowanego serwera;</li><li>• firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.</li></ul> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p>	
Wymagania dodatkowe	<p>Zamawiający wymaga montażu fizycznego serwera wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania oraz serwera fizycznego i 2 maszyn wirtualnych które to wykonawca musi uruchomić na w/w serwerze. Parametry minimalne w/w maszyn wirtualnych zostaną podane na etapie realizacji wdrożenia.</p> <p>W ramach wdrożenia, wykonawca musi sporządzić dokumentację powdrożeniową opisującą wszystkie istotne z punktu działania klastra rekonfiguracje, w tym opis konfiguracji niskopoziomowego zarządzania serwerem.</p>	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



4. Serwer dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Serwer dla Gminnego Ośrodka Pomocy Społecznej	SPEŁNIA TAK /NIE
Obudowa	Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3,5".  Obudowa musi mieć możliwość 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.	SPEŁNIA TAK /NIE
Płyta główna	Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.	SPEŁNIA TAK /NIE
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.8GHz 12MB, dedykowane do pracy z zaoferowanym serwerem	SPEŁNIA TAK /NIE
Pamięć RAM	Minimum 4x 32 GB pamięci RAM RDIMM o częstotliwości taktowania minimum 3200MHz	SPEŁNIA TAK /NIE
Sloty PCI Express	Minimum 3 sloty PCI Express Gen4	SPEŁNIA TAK /NIE
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT	SPEŁNIA TAK /NIE
Dyski Twarde	Zainstalowane minimum 2 dyski SAS o pojemności minimum 2.4TB, 3.5", Hot-Plug  Oraz minimum 2 dyski SATA 480GB SSD.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.	SPEŁNIA TAK /NIE
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.	SPEŁNIA TAK /NIE
Wbudowane porty	Minimum 5 portów USB z czego min. 2 w technologii 3.0  Minimum 1x VGA  Możliwość rozbudowy o port RS-232	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia



Fundusze Europejskie

na Rozwój Cyfrowy

Video	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli	SPEŁNIA TAK /NIE
Zasilanie	Redundantne zasilacze o mocy minimum 700W wraz z kablami zasilającymi.	SPEŁNIA TAK /NIE
Bezpieczeństwo	<ul style="list-style-type: none"><li>• Zintegrowany z płytą główną moduł TPM 2.0</li><li>• Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.</li><li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</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></ul>	SPEŁNIA TAK /NIE
Karta zarządzania	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></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li></ul>	
Oprogramowanie do zarządzania	<ul style="list-style-type: none"><li>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li><li>• integracja z Active Directory</li><li>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li><li>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li><li>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li><li>• Szczegółowy opis wykrytych systemów oraz ich komponentów</li><li>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li><li>• Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.</li><li>• Grupowanie urządzeń w oparciu o kryteria użytkownika</li><li>• Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li><li>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li><li>• Szybki podgląd stanu środowiska</li><li>• Podsumowanie stanu dla każdego urządzenia</li><li>• Szczegółowy status urządzenia/elementu/komponentu</li><li>• Generowanie alertów przy zmianie stanu urządzenia.</li><li>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li><li>• Integracja z service desk producenta dostarczonej platformy sprzętowej</li><li>• Możliwość przejęcia zdalnego pulpitu</li><li>• Możliwość podmontowania wirtualnego napędu</li><li>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li><li>• Możliwość importu plików MIB</li><li>• Przesyłanie alertów „as-is” do innych konsol firm trzecich</li><li>• Możliwość definiowania ról administratorów</li><li>• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li><li>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li><li>• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<ul style="list-style-type: none"><li>Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li></ul>	
Certyfikaty	<ul style="list-style-type: none"><li>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub normami równoważnymi</li><li>Serwer musi posiadać deklarację CE lub normami równoważnymi</li><li>Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.</li><li>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2016, Microsoft Windows 2019.</li></ul>	SPEŁNIA TAK /NIE
Warunki gwarancji	<p>Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta.</p> <p>Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie oświadczenia producenta oferowanego sprzętu.</p> <p>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).</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.</p> <p>Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie:</p> <ul style="list-style-type: none"><li>realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;</li><li>firma serwisująca posiada autoryzację producenta oferowanego serwera;</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	<ul style="list-style-type: none"><li>firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.</li></ul> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p>	
Ilość	1 szt.	SPEŁNIA TAK /NIE

5. Network Attached Storage NAS: Macierz NAS wraz z dyskami dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Network Attached Storage NAS: Macierz NAS wraz z dyskami dla Urzędu Gminy	SPEŁNIA TAK /NIE
Wymagania sprzętowe	<p>Architektura: maksymalnie 2 kontrolery pracujące w trybie Active-Passive</p> <p>Procesor: Procesor o architekturze minimum 64 bit x86 o bazowym taktowaniu nie mniejszym niż 2.4 GHz</p> <p>Procesor liczba rdzeni: Nie mniej niż 4</p> <p>Pamięć RAM: Nie mniej niż 16 GB</p> <p>Liczba zatok na dyski twarde: Minimum 12</p> <p>Obsługiwane dyski twarde: 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD</p> <p>Zainstalowane dyski: minimum 4x 3,5" HDD 16TB SAS 12Gb/s minimum 7200 obr/min., 4x 2,5" SSD 7.68TB SAS 24Gb/s</p> <p>Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 2</p> <p>Porty LAN minimum:</p> <ul style="list-style-type: none"><li>2x 1 GbE RJ45 (na kontroler)</li><li>1x 10GbE RJ45 (na kontroler)</li></ul> <p>Obsługiwane protokoły sieciowe, minimum: SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV.</p> <p>Obsługiwane systemy plików: minimum Btrfs, ext4 (wewnętrzny)</p> <p>Port PCIe: Tak, minimum 1 Gen3 (na kontroler)</p> <p>Typ obudowy: RACK, 2U</p> <p>Dopuszczalna temperatura pracy: od 0 do 35°C</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	Wilgotność względna podczas pracy: 5-95% R.H. Zasilanie: maksymalnie 500W, 100-240 V.	
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108TB Maksymalna liczba wewnętrznych wolumenów: 64TB Minimalna liczba obsługiwanych migawek w systemie: 65 536 Minimalna liczba obiektów iSCSI Target: 256 Minimalna liczba jednostek iSCSI LUN: 512	SPEŁNIA TAK /NIE
Obsługiwane typy macierzy RAID	Podstawowy (basic) JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID F1	SPEŁNIA TAK /NIE
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 16 000 Minimalna liczba grup użytkowników: 512 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń CIFS/NFS/AFP/FTP: 1200	SPEŁNIA TAK /NIE
Wirtualizacja	Obsługa Vmware vSphere, Microsoft Hyper-V, Citrix, OpenStack	SPEŁNIA TAK /NIE
Obsługiwane systemy klienckie	Windows 7 i nowsze, Mac OS X 10.11 i nowszy	SPEŁNIA TAK /NIE
Specyfikacja oprogramowania	Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. System musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych. Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną przez GUI a także agenty na urządzenia PC/MA oraz aplikację mobilną na Android/iOS. Usługa musi umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Omawiana usługa musi umożliwiać pracę z dokumentami biurowym i wspierać wersjonowanie oraz edycję tworzonych plików w czasie rzeczywistym.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



Fundusze Europejskie

na Rozwój Cyfrowy

Zabezpieczenia	Sprzętowy mechanizm szyfrowania, zaporą, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS.	SPEŁNIA TAK /NIE
Gwarancja	Minimum 60 miesięcy gwarancji producenta	SPEŁNIA TAK /NIE
Wymagania dodatkowe	Zamawiający wymaga dostarczenia i wdrożenia sprzętu w zakresie minimum: <ul style="list-style-type: none"><li>Montaż dysków HDD,</li><li>Montaż dysków SSD,</li><li>Inicjalizacja urządzenia</li><li>Aktualizacja firmware,</li><li>Montaż fizyczny w szafie Rack,</li><li>Podłączanie i adresacja IP zgodnie z wytycznymi Zamawiającego,</li><li>Utworzenie grupy dysków,</li><li>Utworzenie wolumenów zgodnie z wytycznymi Zamawiającego,</li><li>Dokumentacja powdrożeniowa</li></ul>	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

6. Network Attached Storage NAS: macierz NAS wraz z dyskami dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Network Attached Storage NAS: macierz NAS wraz z dyskami dla Gminnego Ośrodka Pomocy Społecznej	SPEŁNIA TAK /NIE
Wymagania sprzętowe	Procesor: Procesor o architekturze minimum 64 bit o bazowym taktowaniu nie mniejszym niż 2.2 GHz Procesor liczba rdzeni: Nie mniej niż 4 Pamięć RAM: Nie mniej niż 4 GB Liczba zatok na dyski twarde: Minimum 8 Obsługiwane dyski twarde: 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD Zainstalowane dyski: minimum 4x 3,5" HDD 8TB SAS 6Gb/s minimum 7200 obr/min Możliwość podłączenia modułu rozszerzającego: Tak, maksymalnie 1 Porty LAN minimum: <ul style="list-style-type: none"><li>4x 1 GbE RJ45 (na kontroler)</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	Obsługiwane protokoły sieciowe, minimum: SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV. Obsługiwane systemy plików: minimum <ul style="list-style-type: none"><li>Wewnętrzny: Btrfs, ext4</li><li>Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT</li></ul> Port PCIe: Tak, minimum 1 Gen3 (na kontroler) Typ obudowy: RACK, 2U Dopuszczalna temperatura pracy: od 0 do 35°C Wilgotność względna podczas pracy: 5-95% R.H. Zasilanie: maksymalnie 350W, 100-240 V.	
Zarządzanie pamięcią masową	Maksymalny rozmiar pojedynczego wolumenu: 108TB Maksymalna liczba wewnętrznych wolumenów: 64TB Minimalna liczba obsługiwanych migawek w systemie: 65 536 Minimalna liczba obiektów iSCSI Target: 256 Minimalna liczba jednostek iSCSI LUN: 512	SPEŁNIA TAK /NIE
Obsługiwane typy macierzy RAID	Podstawowy (basic) JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID F1	SPEŁNIA TAK /NIE
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 16 000 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń CIFS/NFS/AFP/FTP: 1000	SPEŁNIA TAK /NIE
Wirtualizacja	Obsługa Vmware vSphere, Microsoft Hyper-V, Citrix, OpenStack	SPEŁNIA TAK /NIE
Obsługiwane systemy klienckie	Windows 7 i nowsze, Mac OS X 10.11 i nowszy	SPEŁNIA TAK /NIE
Specyfikacja oprogramowania	Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. System musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych. Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną przez GUI a także agenty na urządzenia PC/MA oraz aplikację mobilną na Android/iOS. Usługa musi umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Omawiana usługa musi umożliwiać pracę z dokumentami biurowym i wspierać wersjonowanie oraz edycję tworzonych plików w czasie rzeczywistym.	
Zabezpieczenia	Sprzętowy mechanizm szyfrowania, zaporę, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS.	SPEŁNIA TAK /NIE
Gwarancja	Minimum 36 miesięcy gwarancji producenta	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

7. Generator prądu: Agregat prądotwórczy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Generator prądu: Agregat prądotwórczy	SPEŁNIA TAK /NIE
Parametry podstawowe	Agregat prądotwórczy, trójfazowy, zabudowany. Rodzaj: mobilny Moc agregatu minimum: <ul style="list-style-type: none"><li>Moc nominalna: minimum 41 kVA</li><li>Moc maksymalna: minimum 45 kVA</li></ul> Typ agregatu: trójfazowy Sprawność cos Φ minimum: 0.8 Czas pracy przy 75% mocy znamionowej: minimum 10h	SPEŁNIA TAK /NIE
Silnik	Rodzaj paliwa: Olej napędowy (Diesel) Rodzaj silnika: Turbodoładowany z systemem podgrzewu silnika Spalanie:	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><li>Maksymalnie 8 litrów na godzinę (przy 75% mocy maksymalnej)</li><li>Maksymalnie 11 litrów na godzinę (przy 100% mocy maksymalnej)</li></ul> Ilość cylindrów: minimum 4 Wtrysk bezpośredni: tak Turbodoładowanie: tak Konfiguracja silnika: Rzędowy (R4) Rodzaj chłodzenia: cieczą (Agregat posiada chłodnicę) Pojemność skokowa: minimum 3319 cc3 Ilość obrotów na minutę (RPM): minimum 1500 Czujnik ciśnienia oleju: tak Kontrola poziomu paliwa: tak Regulator obrotów silnika: mechaniczny Pojemność miski olejowej: minimum 10l Pojemność chłodziwa: minimum 4l	
Prądnica	Napięcie znamionowe: 400V Współczynnik mocy: cos Φ minimum: 0.8 Moc znamionowa: minimum 45 kVA Częstotliwość: 50 Hz Typ prądnicy: bezszczotkowa Stopień ochrony prądnicy: IP 23 Sprawność prądnicy: minimum 87% Stabilizacja napięcia AVR: tak	SPEŁNIA TAK /NIE
Obudowa	Typ obudowy: zabudowana, wyciszona. Zabudowa odporna na warunki atmosferyczne: tak Poziom ciśnienia akustycznego LWA maksymalnie: 92 db(A) Poziom ciśnienia akustycznego 75 db(A) (pomiar- 1m, otwarta przestrzeń) Pojemność zbiornika paliwa: minimum 80l Uchwyt do przenoszenia dźwigiem: tak	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

Funkcje	Ręczny start Stabilizację napięcia (DSR) Rodzaj rozruchu: Elektryczny	SPEŁNIA TAK /NIE
Sterownik	Wskaźnik poziomu paliwa: tak Kontrola zasilania sieciowego: tak Pomiar wartości prądu w 3 fazach: tak Pomiar wartości napięcia sieci i generatora: tak Pomiar mocy czynnej, biernej i pozornej: tak Licznik czasu pracy: tak Pomiar napięcia akumulatora: tak Magistrala CAN: tak Podłączenie do Internetu: tak, poprzez moduł rozszerzeń (opcjonalne).	SPEŁNIA TAK /NIE
Wymagania dodatkowe	Agregat musi zostać dostarczony w miejsce wskazane przez Zamawiającego na jednoosiowej przyczepie z homologacją która wraz z agregatem stanowi komplet.	SPEŁNIA TAK /NIE
Gwarancja	Gwarancja producenta minimum 12 miesięcy	SPEŁNIA TAK /NIE
Ilość	1 kpl.	SPEŁNIA TAK /NIE

8. UPS stanowiskowy: UPS dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	UPS Stanowiskowy: UPS dla Urzędu Gminy w Rogowie	SPEŁNIA TAK /NIE
Wymagania ogólne dla urządzenia	Technologia: VI (line interactive) Moc pozorna: minimum 850VA Moc rzeczywista: minimum 550W Napięcie wejściowe: 162 ÷ 290 V AC ± 7V Częstotliwość napięcia wejściowego: 40 ÷ 70 Hz ± 1 Hz Zakres napięcia wejściowego: 230 V AC ± 10 % Kształt napięcia wyjściowego (przy pracy rezerwowej/sieciowej): Schodkowa aproksymacja sinusoidy / Tak jak na wejściu	SPEŁNIA TAK /NIE

**Opis przedmiotu zamówienia**

	<p>Progi przełączania sieć- UPS: <math>162 \div 290 \text{ V AC} \pm 7\text{V}</math></p> <p>Czas przełączania sieć- UPS: <math>&lt;6\text{ms}</math></p> <p>Napięcie wyjściowe: <math>\sim 230\text{V} \pm 10\%</math></p> <p>Częstotliwość napięcia wyjściowego: <math>50 / 60 \text{ Hz} \pm 1\%</math></p> <p>Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy</p> <p>Progi przełączania UPS- sieć: <math>\sim 172 \div 280 \text{ V} \pm 7\text{V}</math></p> <p>Przebieżalność: <math>&gt; 110\% - 1 \text{ min}</math> (wyłączenie UPS – praca sieciowa i bateryjna)</p> <p>Zabezpieczenie wyjściowe przeciwzwarcie: elektroniczne</p> <p>Zabezpieczenie wyjściowe przeciążeniowe: elektroniczne</p> <p>Czas podtrzymywania (80%/50% Pmax): minimum 3/8 minut</p> <p>Akumulatory wewnętrzne: minimum 2 szt. 12V5Ah</p>	
<b>Wymagania dodatkowe</b>	<p>Ilość i typ gniazd wyjściowych: minimum 6 x IEC 320 C13 (10A)</p> <p>Sygnalizacja:</p> <ul style="list-style-type: none"> <li>Akustyczna, informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li> <li>Optyczna, dioda sygnalizująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li> </ul> <p>Zimny start: tak</p> <p>Interfejs komunikacyjny: USB HID</p> <p>Automatyczna regulacja napięcia AVR: tak</p>	SPEŁNIA TAK /NIE
<b>Oprogramowanie do zarządzania urządzeniem</b>	<p>Oprogramowania musi zapewniać wsparcie dla systemów: Windows, Linux oraz wirtualizacji Hyper-V, Vmware oraz XenServer.</p> <p>Oprogramowanie musi być dostępne w języku polskim, dostarczone przez producenta oferowanego urządzenia UPS.</p>	SPEŁNIA TAK /NIE
<b>Wymagane certyfikaty</b>	<p>ISO 9001 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu.</p> <p>Deklaracja CE producenta sprzętu.</p>	SPEŁNIA TAK /NIE
<b>Serwis producenta</b>	<p>Autoryzowany serwis producenta zlokalizowany w Polsce.</p> <p>Serwis realizowany w systemie „door-to-door”.</p>	SPEŁNIA TAK /NIE
<b>Gwarancja</b>	<p>Gwarancja producenta minimum 24 miesiące na urządzenia UPS oraz minimum 12 miesięcy na akumulatory.</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



Wymagania dodatkowe	Zamawiający wymaga dostarczenia i wdrożenia sprzętu w zakresie minimum: podłączenie UPS'ów stanowiskowych.	SPEŁNIA TAK /NIE
Ilość	20 sztuk.	SPEŁNIA TAK /NIE

9. UPS stanowiskowy: UPS dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla sprzętu	
Typ	UPS Stanowiskowy: UPS dla Gminnego Ośrodka Pomocy Społecznej w Rogowie	SPEŁNIA TAK /NIE
Wymagania ogólne dla urządzenia	Technologia: VI (line interactive) Moc pozorna: minimum 850VA Moc rzeczywista: minimum 550W Napięcie wejściowe: 162 ÷ 290 V AC ± 7V Częstotliwość napięcia wejściowego: 40 ÷ 70 Hz ± 1 Hz Zakres napięcia wejściowego: 230 V AC ± 10 % Kształt napięcia wyjściowego (przy pracy rezerwowej/sieciowej): Schodkowa aproksymacja sinusoidy / Tak jak na wejściu Progi przełączania sieć- UPS: 162 ÷ 290 V AC ± 7V Czas przełączania sieć- UPS: <6ms Napięcie wyjściowe: ~230V ± 10% Częstotliwość napięcia wyjściowego: 50 / 60 Hz ± 1% Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy Progi przełączania UPS- sieć: ~172 ÷ 280 V ± 7V Przebieżalność: > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) Zabezpieczenie wyjściowe przeciwzwarcowe: elektroniczne Zabezpieczenie wyjściowe przeciążeniowe: elektroniczne Czas podtrzymywania (80%/50% Pmax): minimum 3/8 minut Akumulatory wewnętrzne: minimum 2 szt. 12V5Ah	SPEŁNIA TAK /NIE
Wymagania dodatkowe	Ilość i typ gniazd wyjściowych: minimum 6 x IEC 320 C13 (10A) Sygnaalizacja:	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><li>Akustyczna, informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li><li>Optyczna, dioda sygnalizująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li></ul> Zimny start: tak Interfejs komunikacyjny: USB HID Automatyczna regulacja napięcia AVR: tak	
Oprogramowanie do zarządzania urządzeniem	Oprogramowania musi zapewniać wsparcie dla systemów: Windows, Linux oraz wirtualizacji Hyper-V, Vmware oraz XenServer. Oprogramowanie musi być dostępne w języku polskim, dostarczone przez producenta oferowanego urządzenia UPS.	SPEŁNIA TAK /NIE
Wymagane certyfikaty	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu lub normami równoważnymi Deklaracja CE producenta sprzętu lub normami równoważnymi	SPEŁNIA TAK /NIE
Serwis producenta	Autoryzowany serwis producenta Serwis realizowany w systemie „door-to-door”.	SPEŁNIA TAK /NIE
Gwarancja	Gwarancja producenta minimum 24 miesiące na urządzenia UPS oraz minimum 12 miesięcy na akumulatory.	SPEŁNIA TAK /NIE
Ilość	10 sztuk.	SPEŁNIA TAK /NIE

10. UPS do serwera dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	UPS Serwerowy: UPS dla Urzędu Gminy w Rogowie	SPEŁNIA TAK /NIE
Wymagania ogólne dla urządzenia	Technologia: VI (line interactive) Moc pozorna: minimum 850VA Moc rzeczywista: minimum 550W Napięcie wejściowe: 162 ÷ 290 V AC ± 7V Częstotliwość napięcia wejściowego: 40 ÷ 70 Hz ± 1 Hz	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>Zakres napięcia wejściowego: 230 V AC ± 10 %</p> <p>Kształt napięcia wyjściowego (przy pracy rezerwowej/sieciowej): Schodkowa aproksymacja sinusoidy / Tak jak na wejściu</p> <p>Progi przełączania sieć- UPS: 162 ÷ 290 V AC ± 7V</p> <p>Czas przełączania sieć- UPS: &lt;6ms</p> <p>Napięcie wyjściowe: ~230V ± 10%</p> <p>Częstotliwość napięcia wyjściowego: 50 / 60 Hz ± 1%</p> <p>Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy</p> <p>Progi przełączania UPS- sieć: ~172 ÷ 280 V ± 7V</p> <p>Przebieżalność: &gt; 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna)</p> <p>Zabezpieczenie wyjściowe przeciwzwarcio: elektroniczne</p> <p>Zabezpieczenie wyjściowe przeciążeniowe: elektroniczne</p> <p>Czas podtrzymywania (80%/50% Pmax): minimum 3/8 minut</p> <p>Akumulatory wewnętrzne: minimum 2 szt. 12V 5 Ah</p> <p>Ilość i typ gniazd wyjściowych: minimum 6 x IEC 320 C13 (10A)</p>	
Wymagania dodatkowe	<p>Sygnalizacja:</p> <ul style="list-style-type: none"><li>Akustyczna, informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li><li>Optyczna, dioda sygnalizująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li></ul> <p>Zimny start: tak</p> <p>Interfejs komunikacyjny: USB HID</p> <p>Automatyczna regulacja napięcia AVR: tak</p>	SPEŁNIA TAK /NIE
Oprogramowanie do zarządzania urządzeniem	<p>Oprogramowania musi zapewniać wsparcie dla systemów: Windows, Linux oraz wirtualizacji Hyper-V, Vmware oraz XenServer.</p> <p>Oprogramowanie musi być dostępne w języku polskim, dostarczone przez producenta oferowanego urządzenia UPS.</p>	SPEŁNIA TAK /NIE
Wymagane certyfikaty	<p>ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu lub normami równoważnymi</p> <p>Deklaracja CE producenta sprzętu lub normami równoważnymi</p>	SPEŁNIA TAK /NIE
Serwis producenta	Autoryzowany serwis producenta	

Opis przedmiotu zamówienia



	Serwis realizowany w systemie „door-to-door”.	SPEŁNIA TAK /NIE
Gwarancja	Gwarancja producenta minimum 24 miesiące na urządzenia UPS oraz minimum 12 miesięcy na akumulatory.	SPEŁNIA TAK /NIE
Ilość	2 szt.	SPEŁNIA TAK /NIE

11. UPS do serwera dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla sprzętu	
Typ	UPS Serwerowy: UPS dla Gminnego Ośrodka Pomocy Społecznej w Rogowie	SPEŁNIA TAK /NIE
Wymagania ogólne dla urządzenia	Technologia: VI (line interactive) Moc pozorna: minimum 850VA Moc rzeczywista: minimum 550W Napięcie wejściowe: 162 ÷ 290 V AC ± 7V Częstotliwość napięcia wejściowego: 40 ÷ 70 Hz ± 1 Hz Zakres napięcia wejściowego: 230 V AC ± 10 % Kształt napięcia wyjściowego (przy pracy rezerwowej/sieciowej): Schodkowa aproksymacja sinusoidy / Tak jak na wejściu Progi przełączania sieć- UPS: 162 ÷ 290 V AC ± 7V Czas przełączania sieć- UPS: <6ms Napięcie wyjściowe: ~230V ± 10% Częstotliwość napięcia wyjściowego: 50 / 60 Hz ± 1% Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy Progi przełączania UPS- sieć: ~172 ÷ 280 V ± 7V Przebieżalność: > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) Zabezpieczenie wyjściowe przeciwzwarciowe: elektroniczne Zabezpieczenie wyjściowe przeciążeniowe: elektroniczne Czas podtrzymywania (80%/50% Pmax): minimum 3/8 minut Akumulatory wewnętrzne: minimum 2 szt. 12V 5 Ah Ilość i typ gniazd wyjściowych: minimum 6 x IEC 320 C13 (10A)	SPEŁNIA TAK /NIE
Wymagania dodatkowe	Sygnalizacja:	

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><li>Akustyczna, informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li><li>Optyczna, dioda sygnalizująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu oraz awarii</li></ul> Zimny start: tak Interfejs komunikacyjny: USB HID Automatyczna regulacja napięcia AVR: tak	SPEŁNIA TAK /NIE
Oprogramowanie do zarządzania urządzeniem	Oprogramowania musi zapewniać wsparcie dla systemów: Windows, Linux oraz wirtualizacji Hyper-V, Vmware oraz XenServer. Oprogramowanie musi być dostępne w języku polskim, dostarczone przez producenta oferowanego urządzenia UPS.	SPEŁNIA TAK /NIE
Wymagane certyfikaty	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu lub normami równoważnymi Deklaracja CE producenta sprzętu lub normami równoważnymi	SPEŁNIA TAK /NIE
Serwis producenta	Autoryzowany serwis producenta. Serwis realizowany w systemie „door-to-door”.	SPEŁNIA TAK /NIE
Gwarancja	Gwarancja producenta minimum 24 miesiące na urządzenia UPS oraz minimum 12 miesięcy na akumulatory.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

12. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X. Przełącznik zarządzalny dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X. – Przełącznik zarządzalny dla Urzędu Gminy w Rogowie.	SPEŁNIA TAK /NIE
Obudowa	Do montażu w szafie Rack 19”, o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz.	SPEŁNIA TAK /NIE
Porty	Minimum 48 portów 10/100/1000Mbps RJ45, co najmniej 4 porty SFP+ 10GbE	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia



Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity 176.0 Gbps Forwarding rate minimum 130 Mpps Bufor pakietów 3MB	SPEŁNIA TAK /NIE
Funkcjonalność warstwy II	Flow Control 802.3x Flow Control HOL Blocking Prevention Jumbo Frame - do 9216 bajtów IGMP Snooping IGMP v1/v2 Snooping IGMP v3 awareness do 512 grup IGMP, 128 statycznych adresów multicast, IGMP per VLAN, IGMP Snooping Querier, host-based IGMP Snooping Fast Leave MLD Snooping MLD v1/v2 awareness, 512 grup, 128 statycznych adresów multicast, MLD Snooping per VLAN, host-based MLD Fast Leave, MLD Snooping Querier Wykrywanie pętli (loopback detection) v4.07 802.3ad Agregacja połączeń (do 32 grup na urządzenie / 8 portów na grupę) Port Mirroring do 4 grup, one-to-one, many-to-one. Filtrowanie multicast ERPS (Ethernet Ring Protection Switching)	SPEŁNIA TAK /NIE
Funkcjonalność warstwy III	ARP IPv6 Neighbour Discovery (ND) Minimum 16 interfejsów IP Routing Domyślny Statyczny Routing 64 wejść IPv4, 32 wejścia IPv6 UDP helper	SPEŁNIA TAK /NIE
Zarządzanie	ARP IPv6 Neighbour Discovery (ND) Minimum 16 interfejsów IP Routing Domyślny Statyczny Routing 64 wejść IPv4, 32 wejścia IPv6 UDP helper	SPEŁNIA TAK /NIE
Zgodność z protokołami	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3ae 10 GbE IEEE 802.3x Flow Control	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	IEEE 802.1Q	
Inne	Przystosowanie do pracy w temperaturze od -5 do 50 stopni Celsjusza	SPEŁNIA TAK /NIE
Wymagania dodatkowe	Zamawiający wymaga montażu przełącznika wraz z pełną aktualizacją systemu operacyjnego urządzenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania lub innego dostępnego.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

13. Biblioteka taśmowa dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Biblioteka taśmowa dla Urzędu Gminy w Rogowie	SPEŁNIA TAK /NIE
Obudowa	Obudowa typu Rack o wysokości maksymalnie 1U	SPEŁNIA TAK /NIE
Napęd	Pojedynczy napęd LTO8	SPEŁNIA TAK /NIE
Intefejs	SAS	SPEŁNIA TAK /NIE
Liczba slotów	Urządzenie musi posiadać co najmniej 9 slotów dla nośników	SPEŁNIA TAK /NIE
Dodatkowe	<ul style="list-style-type: none"><li>Urządzenie musi być wyposażone w co najmniej 5 sztuk nośników taśmowych oraz maksymalnie 1 sztukę taśmy czyszczącej.</li><li>Urządzenie musi umożliwiać zarządzanie poprzez przeglądarkę WWW oraz wbudowane klawisze i wyświetlacz LCD.</li><li>Urządzenie musi posiadać wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących długiego przechowywania nienaruszonych danych.</li><li>Urządzenie musi obsługiwać protokoły SNMP oraz IPv6</li></ul>	SPEŁNIA TAK /NIE
Gwarancja	Gwarancja producenta na minimum 36 miesięcy, świadczona przez podmiot posiadający ISO 9001 lub normami równoważnymi oraz ISO-27001 lub normami równoważnymi na świadczenie usług serwisowych. Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie:	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>- realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;</p> <p>- firma serwisująca posiada autoryzację producenta oferowanego serwera;</p> <p>- firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</p> <p>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.</p>	
Wymagania dodatkowe	<p>Zamawiający wymaga dostarczenia i wdrożenia sprzętu w zakresie minimum:</p> <p>Podłączenie i uruchomienie biblioteki taśmowej.</p> <p>Konfiguracja napędu taśmowego z oprogramowaniem do tworzenia kopii zapasowych.</p>	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

14. Oprogramowanie antywirusowe z EDR dla Urzędu Gminy

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie antywirusowe dla Urzędu Gminy w Rogowie	SPEŁNIA TAK /NIE
Wymagania podstawowe	<p>W ramach dostawy Zamawiający wymaga dostarczenia wznowienia aktualnie posiadanej licencji na oprogramowanie antywirusowe WithSecure Elements EPP dla 34 użytkowników wraz z podniesieniem funkcjonalności do wersji z modułem XDR. Dostarczone licencje muszą być ważne do 18.04.2026</p> <p>Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne.</p> <p>Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo:</p> <ul style="list-style-type: none"><li>- wdrożenia</li><li>- skonfigurowania dla wszystkich użytkowników</li><li>- przeszkolenia administratorów dostarczonego oprogramowania, wg ustaleń z Zamawiającym</li></ul>	SPEŁNIA TAK /NIE
Opis równoważności		

Opis przedmiotu zamówienia

Opis technologii	<div><div>1. System musi mieć możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.</div><div>2. Agent instalowany na stacjach końcowych musi posiadać możliwość instalacji z wykorzystaniem mechanizmów dystrybucji przy użyciu usługi katalogowej.</div><div>3. Agent instalowany na stacjach końcowych musi posiadać możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.</div><div>4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.</div><div>5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.</div><div>6. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:<div><div>• dostęp do pliku;</div><div>• tworzenie nowego procesu;</div><div>• nawiązane połączenia sieciowe;</div><div>• wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;</div><div>• zawartość skryptów uruchamianych na monitorowanej stacji.</div></div></div><div>7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń muszą odbywać się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.</div><div>8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.</div><div>9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, musi odbywać się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.</div><div>10. Komunikacja agentów instalowanych na stacjach roboczych, musi wspierać komunikację za pomocą serwera pośredniczącego http (http proxy).</div><div>11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania</div></div>	SPEŁNIA TAK /NIE
------------------	---	------------------

Opis przedmiotu zamówienia

	<p>danych producenta, dane zebrane na stacji końcowej muszą być buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.</p> <p>12. Dane zbierane przez agentów na stacjach końcowych muszą być przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.</p> <p>13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.</p> <p>14. Detekcje muszą być generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.</p> <p>15. Detekcje muszą być generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.</p> <p>16. Detekcje muszą być widoczne w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.</p> <p>17. Detale dotyczące detekcji muszą być przedstawiane w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.</p> <p>18. Rozwiązanie musi posiadać możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.</p> <p>19. Każda detekcja musi zawierać co najmniej następujące informacje:</p> <ul style="list-style-type: none"><li>• Listę urzędzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.</li><li>• Data i czas wystąpienia podejrzanych zdarzeń.</li><li>• Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.</li><li>• Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.</li><li>• Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.</li><li>• Poziom ryzyka, określający istotność danej detekcji.</li></ul>	
--	---	--

Opis przedmiotu zamówienia

	<ul style="list-style-type: none"><li>• Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&amp;C, nieuprawnione wykonanie skryptu).</li></ul> <p>20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne muszą zawierać odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&amp;CK).</p> <p>21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach muszą zawierać odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).</p> <p>22. Rozwiązanie musi umożliwiać oznaczanie wygenerowanych detekcji jako błędne.</p> <p>23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.</p> <p>24. Rozwiązanie musi posiadać możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.</p> <p>25. Rozwiązanie musi pozwalać na dodanie własnego komentarza przy wykrytej detekcji.</p> <p>26. Rozwiązanie musi umożliwiać wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrótnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.</p> <p>27. Rozwiązanie musi pozwalać na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.</p> <p>28. Rozwiązanie musi pozwalać na izolację sieciową komputerów przez administratora.</p> <p>29. Rozwiązanie musi umożliwiać tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.</p> <p>30. Rozwiązanie musi umożliwiać wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług,</p>	
--	---	--

Opis przedmiotu zamówienia

	<p>umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.</p> <p>31. Rozwiązanie musi umożliwiać tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.</p> <p>32. Rozwiązanie musi pozwalać na eksport raportów, w postaci plików PDF.</p> <p>33. Rozwiązanie musi wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.</p> <p>34. Konsola centralnego zarządzania, musi oferować interfejs w języku Polskim.</p> <p>35. Konsola zarządzająca musi być wyposażona w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.</p> <p>36. Rozwiązanie musi umożliwiać wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.</p> <p>37. Konsola musi być wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.</p> <p>38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR musi zawierać informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.</p> <p>39. Ochrona antywirusowa musi być realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.</p> <p>40. Rozwiązanie musi posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.</p> <p>41. Rozwiązanie musi wspierać technologię Antimalware Scan Interface (AMSI)</p> <p>42. Rozwiązanie musi umożliwiać wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.</p> <p>43. W momencie wykrycia infekcji rozwiązanie musi automatycznie starać się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.</p>	
--	--	--



Opis przedmiotu zamówienia

	<div>44. Rozwiązanie musi posiadać możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.</div> <div>45. Rozwiązanie musi chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.</div> <div>46. Rozwiązanie musi posiadać mechanizmy skanujące dyski sieciowe.</div> <div>47. Skanowanie dysków sieciowych musi być możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.</div> <div>48. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.</div> <div>49. Rozwiązanie musi posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.</div> <div>50. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.</div> <div>51. Aktualizacje baz definicji wirusów musi być dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.</div> <div>52. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.</div> <div>53. Rozwiązanie musi posiadać możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.</div> <div>54. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, musi następować w sposób automatyczny, niewidoczny dla użytkownika końcowego.</div> <div>55. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie może wymagać dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.</div> <div>56. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.</div>	
--	--	--



Opis przedmiotu zamówienia

	<div>57. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.</div> <div>58. Rozwiązanie musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</div> <div>59. Rozwiązanie musi posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</div> <div>60. Rozwiązanie musi posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.</div> <div>61. Rozwiązanie musi posiadać możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.</div> <div>62. Rozwiązanie musi posiadać możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.</div> <div>63. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.</div> <div>64. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie może wymagać zatrzymania procesu skanowania na jakimkolwiek systemie.</div> <div>65. Rozwiązanie musi posiadać funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym</div> <div>66. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</div> <div>67. Aktualizacja mechanizmów skanujących i definicji wirusów nie może wymagać konieczności restartu systemu operacyjnego.</div> <div>68. Rozwiązanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów.</div> <div>69. Rozwiązanie musi umożliwiać wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.</div>	
--	--	--

Opis przedmiotu zamówienia

	<div>70. Rozwiązanie musi posiadać mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.</div> <div>71. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.</div> <div>72. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.</div> <div>73. Rozwiązanie musi posiadać możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.</div> <div>74. Rozwiązanie musi posiadać możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.</div> <div>75. Rozwiązanie musi posiadać możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.</div> <div>76. Rozwiązanie musi posiadać możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.</div> <div>77. Rozwiązanie musi automatycznie powiadamiać użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.</div> <div>78. Rozwiązanie musi posiadać możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.</div> <div>79. Rozwiązanie musi posiadać możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.</div> <div>80. Rozwiązanie musi umożliwiać blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</div>	
--	--	--

Opis przedmiotu zamówienia



	<div>81. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.</div> <div>82. Rozwiązanie musi posiadać możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.</div> <div>83. Rozwiązanie musi być wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.</div> <div>84. Rozwiązanie musi posiadać możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.</div> <div>85. Rozwiązanie musi umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.</div> <div>86. Oprogramowanie musi zapewniać co najmniej 30 kategorii klasyfikacji witryn WWW.</div> <div>87. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, musi być powiadamiany o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.</div> <div>88. Rozwiązanie musi umożliwiać blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.</div> <div>89. Rozwiązanie musi posiadać wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.</div> <div>90. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie musi blokować możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.</div> <div>91. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie musi automatycznie blokować zdalny dostęp do hosta za pomocą takich narzędzi jak minimum pulpit zdalny, TeamViewer .</div> <div>92. Kontrola połączenia musi umożliwiać zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.</div>	
--	--	--

Opis przedmiotu zamówienia

	<p>93. Rozwiązanie musi posiadać wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.</p> <p>94. Rozwiązanie musi posiadać funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.</p> <p>95. Profile bezpieczeństwa zapory ogniowej muszą zawierać predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.</p> <p>96. Rozwiązanie musi pozwalać na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.</p> <p>97. Rozwiązanie musi posiadać możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).</p> <p>98. Rozwiązanie musi umożliwiać stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.</p> <p>99. Rozwiązanie musi być wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.</p> <p>100. Mechanizm aktualizacji aplikacji (patch management) nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.</p> <p>101. Moduł aktualizacji aplikacji musi okresowo skanować aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.</p> <p>102. Moduł aktualizacji aplikacji musi pełnić role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.</p> <p>103. Administrator musi posiadać możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.</p>	
--	---	--

Opis przedmiotu zamówienia

	<p>104.Administrator musi posiadać możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.</p> <p>105.Mechanizm aktualizacji aplikacji musi umożliwiać automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.</p> <p>106.W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator musi posiadać możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.</p> <p>107.Administrator konsoli zarządzającej musi mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.</p> <p>108.Mechanizm aktualizacji aplikacji (patch management) nie może wymagać uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.</p> <p>109.Administrator musi mieć możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.</p> <p>110.Rozwiązanie musi umożliwiać wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.</p> <p>111.System centralnego zarządzania musi prezentować niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.</p> <p>112.Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.</p> <p>113.Mechanizm kontroli urządzeń zewnętrznych musi wspierać m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.</p> <p>114.Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.</p>	
--	--	--

**Opis przedmiotu zamówienia**

- |  |   |  |
|--|---|--|
|  | <p>115. Lista urządzeń zaufanych musi być tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.</p> <p>116. Rozwiązanie musi posiadać możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.</p> <p>117. Mechanizm kontroli urządzeń musi umożliwiać blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.</p> <p>118. Rozwiązanie musi posiadać opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.</p> <p>119. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.</p> <p>120. Rozwiązanie musi posiadać możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker</p> <p>121. Rozwiązanie musi pozwalać na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.</p> <p>122. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator musi posiadać możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.</p> <p>123. Rozwiązanie musi pozwalać na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.</p> <p>124. Administrator w konsoli zarządzającej musi posiadać dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.</p> <p>125. Rozwiązanie musi posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.</p> <p>126. Mechanizm w swoim działaniu musi wykorzystywać własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)</p> <p>127. W przypadku wykrycia szkodliwego działania ransomware, moduł musi blokować aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.</p> |  |
|--|---|--|

**Opis przedmiotu zamówienia**

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>128.Moduł przywracania plików zaszyfrowanych musi umożliwiać działanie w trybie monitorowania, bez podejmowania reakcji.</p> <p>129.Administrator musi mieć możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.</p> <p>130.Administrator musi posiadać możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.</p> <p>131.Rozwiązanie musi być wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.</p> <p>132.Moduł musi posiadać możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.</p> <p>133.Administrator musi posiadać możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.</p> <p>134.Rozwiązanie musi posiadać możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów muszą mieć możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.</p> <p>135.Rozwiązanie musi potrafić automatycznie wykrywać zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz musi posiadać możliwość wskazania zaufanych aplikacji przez administratora.</p> <p>136.Rozwiązanie musi posiadać funkcjonalność kontroli uruchamianych aplikacji.</p> <p>137.Tryb kontroli aplikacji musi umożliwiać uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.</p> <p>138.System musi posiadać możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.</p> <p>139.Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.</p> <p>140.Na wspieranych systemach Windows rozwiązanie musi pozwalać na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.</p>	
--	--	--



Opis przedmiotu zamówienia

	<p>141.Administrator musi posiadać w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN</p> <p>142.Rozwiązanie musi pozwalać na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)</p> <p>143.Administrator musi mieć możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.</p> <p>144.Rozwiązanie musi pozwalać na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).</p> <p>145.Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.</p>	
Centralna administracja	<p>1. Portal musi umożliwiać zarządzania w języku polskim.</p> <p>2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi musi odbywać się w formie zaszyfrowanej.</p> <p>3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie może być wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.</p> <p>4. Interfejs zarządzania musi posiadać funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.</p> <p>5. Interfejs musi być wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.</p> <p>6. Wykresy muszą być interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<div>7. Rozwiązanie musi posiadać dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.</div> <div>8. Rozwiązanie musi posiadać możliwość eksportu listy wszystkich hostów do pliku CSV.</div> <div>9. Administrator musi mieć możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.</div> <div>10. Administrator musi mieć możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.</div> <div>11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.</div> <div>12. Rozwiązanie musi posiadać dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.</div> <div>13. Rozwiązanie musi zapewniać możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.</div> <div>14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego muszą zawierać liczbę i typ hostów, na których został wykryty brak danej poprawki.</div> <div>15. Po wskazaniu danej poprawki administrator musi posiadać możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.</div> <div>16. Administrator musi mieć możliwość wglądu w historię instalowanych poprawek na chronionych hostach.</div> <div>17. Rozwiązanie musi posiadać moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.</div> <div>18. Rozwiązanie musi umożliwiać tworzenie raportów zgodnie z harmonogramem i wysyłanie na wskazane adresy email.</div> <div>19. Rozwiązanie musi posiadać wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.</div>	
--	---	--

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div><div>20. Administrator musi mieć możliwość widzenia w konsoli informacji dotyczących produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.</div><div>21. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.</div><div>22. Dodanie klucza licencyjnego musi skutkować pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.</div><div>23. Rozwiązanie musi mieć możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.</div><div>24. System musi pozwalać na przypisywanie profili do pojedynczych hostów lub grup.</div><div>25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do usługi katalogowej.</div><div>26. W przypadku automatycznego przypisywania profili, system musi pozwalać na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.</div><div>27. System musi zapewniać możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.</div><div>28. Rozwiązanie musi pozwalać administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.</div><div>29. Z poziomu portalu zarządzającego musi istnieć możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.</div><div>30. Pliki instalacyjne muszą mieć postać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.</div><div>31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.</div><div>32. Administrator musi posiadać możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.</div></div>	
--	---	--



Opis przedmiotu zamówienia

	<p>33. Administrator musi posiadać do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.</p> <p>34. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.</p> <p>35. Konsola musi posiadać możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.</p> <p>36. W ramach posiadanych licencji musi istnieć możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.</p>	
Ilość	1 szt.	SPEŁNIA TAK /NIE

15. Oprogramowanie antywirusowe: Oprogramowanie antywirusowe dla telefonów dla Urzędu Gminy

Nazwa	Minimalne wymagania dla sprzętu	
Typ	Oprogramowanie antywirusowe: Oprogramowanie antywirusowe dla telefonów dla Urzędu Gminy	SPEŁNIA TAK /NIE
Informacje podstawowe	W ramach dostawy Zamawiający wymaga dostarczenia oprogramowania niezbędnego do ochrony urządzeń mobilnych dla 34 użytkowników. Licencja musi obowiązywać do minimum 18.04.2026.	SPEŁNIA TAK /NIE
Wspierane systemy operacyjne	<ul style="list-style-type: none"><li>Android 11 i nowsze wersje</li><li>iOS 15 lub nowszy</li></ul>	SPEŁNIA TAK /NIE
Funkcje bramki sieciowej	<p>1. Oprogramowanie musi mieć możliwość sprawdzenia każdej odwiedzonej witryny.</p> <p>2. Oprogramowanie musi zapewniać usługę reputacji adresów URL aby sprawdzić jakiego rodzaju treści dostarczają.</p>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div>3. Oprogramowanie musi mieć możliwość całkowitego blokowania stron.</div> <div>4. Oprogramowanie musi posiadać funkcję opcjonalnego blokowania treści dla dorosłych lub treści hazardowych.</div> <div>5. Oprogramowanie musi zapewniać architekturę która eliminuje opóźnienia i buforowanie.</div> <div>6. Oprogramowanie musi mieć możliwość przesyłania określonych witryn do konsoli administratora, administrator może decydować o kolejnych działaniach.</div> <div>7. Oprogramowanie musi umożliwiać ograniczanie widoczności adresu URL ze względu na lokalne przepisy dotyczące prywatności pracowników.</div> <div>8. Brama sieciowa musi zapewniać zwiększone bezpieczeństwo i zaawansowaną kontrolę zarówno dla urządzeń z systemem iOS jak i Android.</div>	
Funkcje ochrony chmurowej	<div>1. Oprogramowanie musi wykorzystać analizę zagrożeń w czasie rzeczywistym, zapewniając identyfikację, analizę i zapobieganie wszystkim nowym lub pojawiającym się zagrożeniom w ciągu kilku minut.</div> <div>2. Oprogramowanie musi umożliwiać skanowanie i weryfikację reputacji pobranych aplikacji i plików.</div> <div>3. Uruchamianie złośliwych plików musi być blokowane a nieznane pliki lub aplikacje muszą być przesyłane w celu głębszej analizy.</div>	SPEŁNIA TAK /NIE
Ochrona aplikacji	<div>1. Urządzenia mobilne muszą być automatycznie chronione chronione gdy brama sieciowa jest włączona.</div> <div>2. Oprogramowanie musi zapewniać funkcję skanowania ruchu na poziomie sieci.</div> <div>3. Bezpieczeństwo nie może być ograniczane przez ograniczone zasoby urządzeń mobilnych.</div> <div>4. Procesy wymagające dużych zasobów nie mogą mieć wpływu na wydajność urządzenia i żywotność baterii.</div> <div>5. Skanowanie na poziomie sieci musi zapobiegać kontaktowi ze złośliwą zawartością.</div>	SPEŁNIA TAK /NIE
Ochrona przeglądania	<div>1. Ochrona przeglądania musi być w pełni niezależna od przeglądarki.</div> <div>2. System musi chronić użytkowników końcowych którzy zostali oszukani w celu uzyskania dostępu do pozornie legalnych witryn phishingowych, uzyskania dostępu do złośliwych witryn za pośrednictwem łącza e-mail lub zainfekowania poprzez złośliwe reklamy stron trzecich w legalnych witrynach.</div> <div>3. Ochrona przeglądania musi wykorzystywać analizę zagrożeń w czasie rzeczywistym i pobierać najnowsze wyniki kontroli reputacji witryn internetowych</div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Dodatkowe funkcje	1. Oprogramowanie musi mieć minimalny wpływ na wydajność urządzenia i żywotność baterii. 2. System musi stosować kompresje ruchu i zapobiegać śledzeniu i reklamom online. 3. Oprogramowanie musi być możliwe do zainstalowania przez oprogramowanie do zarządzania urządzeniami mobilnymi (MDM) innych firm.	SPEŁNIA TAK /NIE
Zarządzanie	1. System musi mieć możliwość zarządzania w chmurze. 2. System musi mieć możliwość pełnej widoczności i kontroli nad ustawieniami zabezpieczeń.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

16. Oprogramowanie antywirusowe: Oprogramowanie antywirusowe dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie antywirusowe: Oprogramowanie antywirusowe dla GOPS	SPEŁNIA TAK /NIE
Wymagania podstawowe	<p>W ramach dostawy Zamawiający wymaga dostarczenia wznowienia aktualnie posiadanej licencji na oprogramowanie antywirusowe ESET PROTECT ESSENTIAL (obejmującej 16 stanowisk). Dodatkowo w ramach realizacji przedmiotu zamówienia, Zamawiający wymaga podniesienia funkcjonalności posiadanej licencji do oprogramowania z wbudowanym modułem dotyczącym zarządzania podatnościami wraz z rozszerzeniem ilości licencji do 26 stanowisk. Dostarczone licencje muszą być ważne do 18.04.2026</p> <p>Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne.</p> <p>Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo:</p> <ul style="list-style-type: none"><li>- wdrożenia</li><li>- skonfigurowania dla wszystkich użytkowników</li><li>- przeszkolenia administratorów dostarczonego oprogramowania, wg ustaleń z Zamawiającym</li></ul>	SPEŁNIA TAK /NIE
OPIS RÓWNOWAŻNOŚCI- wymagania minimalne:		
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.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div>4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.</div> <div>5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.</div> <div>6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.</div> <div>7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</div> <div>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 uprawnienia: odczyt, użyj, zapisz oraz brak.</div> <div>9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</div> <div>10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</div> <div>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.</div> <div>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.</div>	
Ochrona stacji roboczych	<div>1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11) posiadane przez Zamawiającego.</div> <div>2. Rozwiązanie musi wspierać architekturę ARM64.</div> <div>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</div> <div>4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</div> <div>5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</div>	SPEŁNIA TAK /NIE

**Opis przedmiotu zamówienia**

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
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.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
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).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
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.
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.
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.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,



Opis przedmiotu zamówienia



	<ul style="list-style-type: none"><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></ul>	
--	--	--

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"><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 wyposażone 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>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p><i>Dodatkowe wymagania dla ochrony serwerów Windows:</i></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 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><i>Dodatkowe wymagania dla ochrony serwerów Linux:</i></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.</p> <p>Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii</p>	
--	--	--

Opis przedmiotu zamówienia



Fundusze Europejskie

na Rozwój Cyfrowy

	jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.	
Szyfrowanie	<div>1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.</div> <div>2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).</div> <div>3. plikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.</div> <div>4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.</div>	SPEŁNIA TAK /NIE
Ochrona urządzeń mobilnych opartych o system Android	<div>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</div> <div>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</div> <div>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</div> <div>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</div> <div>5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:<ul style="list-style-type: none"><li>• usunięcie zawartości urządzenia,</li><li>• przywrócenie urządzenie do ustawień fabrycznych,</li><li>• zablokowania urządzenia,</li><li>• uruchomienie sygnału dźwiękowego,</li><li>• lokalizację GPS.</li></ul></div> <div>6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</div> <div>7. Rozwiązanie musi posiadać możliwość blokowania aplikacji w oparciu o:<ul style="list-style-type: none"><li>• nazwę aplikacji,</li><li>• nazwę pakietu,</li><li>• kategorię sklepu Google Play,</li><li>• uprawnienia aplikacji,</li><li>• pochodzenie aplikacji z nieznanego źródła.</li></ul></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

Ochrona serwera pocztowego MS Exchange	<div><div>1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.</div><div>2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.</div><div>3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.</div><div>4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.</div><div>5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.</div><div>6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.</div><div>7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.</div><div>8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.</div><div>9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.</div><div>10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).</div><div>11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</div></div>	SPEŁNIA TAK /NIE
Sandbox w chmurze	<div><div>1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</div><div>2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.</div><div>3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.</div><div>4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.</div><div>5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.</div><div>6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub</div></div>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>folderów z przesyłania.</p> <p>7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.</p> <p>8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.</p> <p>9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.</p> <p>10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.</p> <p>11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi mieć możliwość podejrzenia jakie pliki zostały wysłane do analizy oraz przez kogo.</p> <p>12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:</p> <ul style="list-style-type: none"><li>• Czysty,</li><li>• Podejrzany,</li><li>• Bardzo podejrzany,</li><li>• Szkodliwy.</li></ul> <p>13. 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> <p>14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.</p> <p>15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.</p>	
<p>Ochrona usługi Microsoft 365</p>	<p>1. Rozwiązanie musi obejmować ochronę usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.</p> <p>2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.</p> <p>3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.</p> <p>4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.</p>	<p>SPEŁNIA TAK /NIE</p>

**Opis przedmiotu zamówienia**

5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
- użytkowników, otrzymujących najwięcej spamu,
  - użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
  - użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
  - kont użytkowników, które mogą być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
- jaka ilość wiadomości została przeskanowana,
  - wynik skanowania poszczególnych wiadomości,
  - czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
- zagrożeniach, które zostały wykryte,
  - na jakim koncie zostały wykryte,
  - jakie zagrożenie zostało wykryte,
  - podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
- wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
  - wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
  - dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.

Opis przedmiotu zamówienia



Fundusze Europejskie

na Rozwój Cyfrowy

	<p>16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.</p> <p>17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.</p> <p>18. Rozwiązanie musi posiadać możliwość przysyłania powiadomień e-mail z funkcją wyboru preferowanego języka.</p>	
<p><b>Moduł zarządzania podatnościami i aktualizacjami</b></p>	<p>1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.</p> <p>2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.</p> <p>3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.</p> <p>5. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.</p> <p>6. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:</p> <ul style="list-style-type: none"><li>• nazwę aplikacji lub systemu operacyjnego</li><li>• punktację CVSS</li><li>• opis wykrytej podatności</li><li>• wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta</li></ul> <p>7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.</p> <p>8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.</p> <p>9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.</p>	<p>SPEŁNIA TAK /NIE</p>



Opis przedmiotu zamówienia



	10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. 11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze. 12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania. 13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania. 14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.	
Ilość	1 szt.	SPEŁNIA TAK /NIE

17. Oprogramowanie do wykonywania kopii zapasowych dla Urzędu Gminy

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie do wykonywania kopii zapasowych typ 1 dla Urzędu Gminy w Rogowie	SPEŁNIA TAK /NIE
Wymagania funkcjonalne	Oprogramowanie musi spełniać następujące funkcjonalności w zakresie minimum: Musi dawać możliwość backupu minimum 60 komputerów, 3 serwerów oraz 2 hostów wirtualizacji. Oprogramowanie musi działać w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich Program serwerowy musi być kompatybilny co najmniej z systemami: Windows 10; Windows 11; Microsoft Windows Server 2019, 2022, Linux Program kliencki musi być kompatybilny co najmniej z systemami: Windows 10; Windows 11; Microsoft Windows Server 2 2019, 2022, Linux, Musi dawać możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)	SPEŁNIA TAK /NIE

**Opis przedmiotu zamówienia**

Musi dawać możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)

Musi przeprowadzać automatyczny backup przy wyłączeniu komputera

Musi dawać możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ?

Musi umożliwiać backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)

Musi umożliwiać backup baz danych i plików poczty w trybie online i offline

Musi dawać możliwość tworzenia kopii rotacyjnych (wersjonowanie)

Musi przeprowadzać zapis archiwów co najmniej w otwartym formacie (ZIP 64-bit)

Musi umożliwiać backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V

Musi pozwalać na odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)

Musi pozwalać na bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej

Musi pozwalać na odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych

Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO

Musi umożliwiać kompresję po stronie stacji roboczej

Musi umożliwiać replikację archiwów na dodatkowy dysk twardy, NAS, serwer FTP,

Musi umożliwiać replikację na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD.

Musi dawać możliwość centralnego sterowania całym Systemem z jednego miejsca

Musi pozwalać na transparentną archiwizację wykonywaną w tle, która nie jest odczuwalna przez pracowników

Musi dawać możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN

Musi umożliwiać wysyłanie alertów administracyjnych na e-mail

Musi dawać możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych

Musi pozwalać na generowanie raportów podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki

Opis przedmiotu zamówienia

	Musi dawać możliwość przeprowadzania automatycznej aktualizacji oprogramowania na komputerach zdalnych	
Licencja	W ramach dostawy wymagane jest dostarczenie licencji bezterminowej (licencja nie może być ograniczona czasowo) z dodatkowym wsparciem technicznym producenta na okres 12 miesięcy dla minimum: <ul style="list-style-type: none"><li>25 komputerów</li><li>3 serwerów</li><li>2 serwerów wirtualnych</li></ul>	SPEŁNIA TAK /NIE
Dodatkowe wymagania	Interfejs, instrukcja i pomoc techniczna w języku polskim. Zamawiający wymaga wdrożenia rozwiązania w zakresie instalacji oprogramowania na wskazanych komputerach.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

18. Oprogramowanie do wykonywania kopii zapasowych dla Gminnego Ośrodka Pomocy Społecznej

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie do wykonywania kopii zapasowych typ 1 dla Gminnego Ośrodka Pomocy Społecznej w Rogowie	SPEŁNIA TAK /NIE
Wymagania funkcjonalne	Oprogramowanie musi spełniać następujące funkcjonalności w zakresie minimum: Musi dawać możliwość backupu minimum 15 komputerów, 1 serwera oraz 2 hostów wirtualizacji. Oprogramowanie musi działać w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich Program serwerowy musi być kompatybilny co najmniej z systemami: Windows 10; Windows 11; Microsoft Windows Server 2019, 2022, Linux Program kliencki musi być kompatybilny co najmniej z systemami: Windows 10; Windows 11; Microsoft Windows Server 2 2019, 2022, Linux,	SPEŁNIA TAK /NIE

**Opis przedmiotu zamówienia**

Musi dawać możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)

Musi dawać możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)

Musi przeprowadzać automatyczny backup przy wyłączaniu komputera

Musi dawać możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ?

Musi umożliwiać backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)

Musi umożliwiać backup baz danych i plików poczty w trybie online i offline

Musi dawać możliwość tworzenia kopii rotacyjnych (wersjonowanie)

Musi przeprowadzać zapis archiwów co najmniej w otwartym formacie (ZIP 64-bit)

Musi umożliwiać backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V

Musi pozwalać na odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)

Musi pozwalać na bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej

Musi pozwalać na odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych

Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO

Musi umożliwiać kompresję po stronie stacji roboczej

Musi umożliwiać replikację archiwów na dodatkowy dysk twardy, NAS, serwer FTP,

Musi umożliwiać replikację na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD.

Musi dawać możliwość centralnego sterowania całym Systemem z jednego miejsca

Musi pozwalać na transparentną archiwizację wykonywaną w tle, która nie jest odczuwalna przez pracowników

Musi dawać możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN

Musi umożliwiać wysyłanie alertów administracyjnych na e-mail

Musi dawać możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych

Opis przedmiotu zamówienia



	Musi pozwalać na generowanie raportów podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki Musi dawać możliwość przeprowadzania automatycznej aktualizacji oprogramowania na komputerach zdalnych	
Licencja	W ramach dostawy wymagane jest dostarczenie licencji bezterminowej (licencja nie może być ograniczona czasowo) z dodatkowym wsparciem technicznym producenta na okres 12 miesięcy dla minimum: <ul style="list-style-type: none"><li>15 komputerów</li><li>1 serwera</li><li>2 serwerów wirtualnych</li></ul>	SPEŁNIA TAK /NIE
Dodatkowe wymagania	Interfejs, instrukcja i pomoc techniczna w języku polskim	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

19. Oprogramowanie SIEM (Security Information and Event Management) dla Urzędu Gminy

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie SIEM: Security Information and Event Management	SPEŁNIA TAK /NIE
Wymagania podstawowe	Wymagane jest dostarczenie oprogramowania posiadającego poniższą funkcjonalność: Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń: <ul style="list-style-type: none"><li>Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna.</li><li>Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (usługą katalogową) lub ręcznie przez definiowanie kont w samym rozwiązaniu.</li><li>System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	<ul style="list-style-type: none"><li>• System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.</li><li>• System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z dowolną przeglądarką WWW.</li><li>• System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.</li><li>• System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych</li></ul> <p>W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń: (dashboardów).</p> <ul style="list-style-type: none"><li>• Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynach wirtualnych.</li><li>• Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca proponuje rozwiązanie pozwalające na usynchronizowanie zegarów czasów sieci Zamawiającego.</li><li>• Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.</li><li>• Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktywności prawnych i dobrych praktyk występujących w środowisku Zamawiającego.</li><li>• Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:<ol style="list-style-type: none"><li>1. Urządzenie klasy UTM</li><li>2. Przełączniki zarządzalne</li><li>3. Serwery fizyczne</li></ol></li></ul>	
--	--	--

Opis przedmiotu zamówienia



	<div>4. Serwery wirtualizacji</div> <div>5. Stacje robocze</div> <div>6. Aplikację centralnego zarządzania posiadanego antywirusa łącznie z modułem XDR</div> <div>7. Apliację do monitorowania infrastruktury informatycznej dla Zamawiającego</div> <ul style="list-style-type: none"><li>• Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.</li><li>• Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.</li><li>• Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.</li><li>• Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.</li><li>• Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.</li><li>• Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.</li></ul>	
<div>Gwarancja i asysta techniczna</div>	<p>Zamawiający wymaga, aby Wykonawca w czasie do 18.04.2026 od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.</p> <p>Zamawiający wymaga, aby Wykonawca w okresie do 18.04.2026 od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.</p> <p>Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.</p> <p>Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.</p>	<div>SPEŁNIA TAK /NIE</div>
<div>Ilość</div>	<div>1 szt.</div>	<div>SPEŁNIA TAK /NIE</div>

20. Oprogramowanie przeciwdziałające wyciekowi danych DLP- Data Leak Prevention dla Urzędu Gminy i Gminnego Ośrodka Pomocy

Spółecznej

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie przeciwdziałającemu wyciekowi danych DLP - Data Leak Prevention dla Urzędu Gminy i Ośrodka Pomocy Społecznej w Rogowie	SPEŁNIA TAK /NIE
Wymagania ogólne	<p>Zamawiający wymaga dostarczenia licencji o minimalnych wymaganiach:</p> <p>System musi być wspierany przez:</p> <ul style="list-style-type: none"><li>a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi</li><li>b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi</li><li>c. MacOS 12 lub nowszy.</li></ul> <p>Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.</p> <p>Serwer administracyjny musi obsługiwać bazy danych:</p> <ul style="list-style-type: none"><li>a. MS SQL Server 2016 lub nowsze,</li><li>b. MS SQL Express,</li><li>c. Pomoc i dokumentacja programu dostępne w języku angielskim.</li></ul> <p>Konsola administracyjna i komunikaty klienta muszą być w języku polskim.</p> <p>Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.</p> <p>Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.</p> <p>Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.</p> <p>Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.</p> <p>Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.</p> <p>Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.</p> <p>Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.</p>	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia



	<p>Administrator musi mieć możliwość, aby tworzyć, usuwać i konta administratorów w konsoli programu.</p> <p>Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).</p> <p>Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.</p> <p>System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.</p> <p>Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.</p> <p>Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.</p> <p>Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.</p> <p>Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.</p> <p>Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.</p> <p>Dashboardsy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.</p> <p>Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.</p> <p>Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.</p> <p>Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.</p>	
--	--	--

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.</p> <p>Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.</p> <p>Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.</p> <p>Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.</p> <p>Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.</p> <p>Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.</p> <p>Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.</p> <p>System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.</p>	
Licencja	<p>Zamawiający wymaga w ramach dostawy do dostarczenia licencji bezterminowych oprogramowania klasy DLP dla minimum 60 użytkowników wraz ze wsparciem obowiązującym do dnia minimum 18.04.2026</p>	SPEŁNIA TAK /NIE
Wdrożenie	<p>Zamawiający wymaga wdrożenia rozwiązania w zakresie minimum:</p> <ul style="list-style-type: none"><li>• Instalacja oprogramowania DLP</li><li>• Instalacja konsoli zarządzającej</li><li>• Przeprowadzenie logowania do konsoli zarządzającej</li><li>• Konfiguracja SMTP</li><li>• Podłączenie do infrastruktury posiadanej przez Zamawiającego (Active Directory)</li><li>• Wygenerowanie agenta rozwiązania DLP oraz przeprowadzenie instalacji na środowiskach testowych wybranych przed wdrożeniem</li><li>• Przypisanie licencji</li><li>• Konfiguracja raportowania i monitorowania</li><li>• Utworzenie stref bezpiecznych i niebezpiecznych</li><li>• Instalacja klienta na stacjach z zainstalowanym agentem</li><li>• Utworzenie reguł DLP wcześniej skonsultowanych z Zamawiającym</li></ul>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia



	• Wykonanie testów	
Ilość	1 szt.	SPEŁNIA TAK /NIE

21. Oprogramowanie do monitorowania infrastruktury informatycznej dla Urzędu Gminy

Nazwa	Minimalne wymagania dla oprogramowania	
Typ	Oprogramowanie do monitorowania infrastruktury informatycznej dla Urzędu Gminy- wymagania minimalne.	SPEŁNIA TAK /NIE
Wymagania podstawowe	W ramach dostawy Zamawiający wymaga dostarczenia wznowienia serwisu aktualnie posiadanej licencji na oprogramowanie do monitorowania infrastruktury informatycznej IT Manager dla minimum 34 stanowisk. Dostarczone licencje muszą być ważne do18.04.2026 Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: - wdrożenia - skonfigurowania dla wszystkich użytkowników - przeszkolenia administratorów dostarczonego oprogramowania, wg ustaleń z Zamawiającym	SPEŁNIA TAK /NIE
Opis równoważności		
Informacje ogólne	1. Oprogramowanie musi umożliwiać zautomatyzowaną oraz niewidoczną dla użytkownika instalację klienta. 2. Oprogramowanie musi wykorzystywać zasady systemów katalogowania lub skryptów instalacyjnych. 3. Konsola zarządzająca administratora musi być zabezpieczona fizycznym kluczem HASP. 4. Konsola zarządzająca musi składać się z modułów z których każdy odpowiada za inne funkcje.	SPEŁNIA TAK /NIE
Zarządzanie infrastrukturą IT	1. Moduł musi pozwalać na centralne zarządzanie zasobami. 2. Moduł musi posiadać wbudowany kreator umożliwiający tworzenie dowolnych zasobów. 3. Moduł musi umożliwiać inwentaryzację konfiguracji komputerów. 4. Moduł musi posiadać bazę konfiguracji komputerów oraz oprogramowania.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	<div>5. Moduł musi umożliwiać zarządzanie legalnością oprogramowania.</div> <div>6. Moduł musi umożliwiać zarządzanie zasobami oraz użytkownikami.</div> <div>7. Moduł musi umożliwiać stały monitoring infrastruktury komputerowej: konfiguracji sprzętowej i oprogramowania.</div> <div>8. Moduł musi umożliwiać w sposób przejrzysty i ergonomiczny zarządzanie komputerami w firmie.</div> <div>9. Interfejs konsoli musi umożliwiać prezentacje stanowisk w różnych formach: listy, struktury organizacyjnej, struktury lokalizacyjnej lub sieciowej.</div> <div>10. System musi posiadać wbudowany mechanizm informując administratorów o wykrytych nieprawidłowościach.</div> <div>11. Moduł musi umożliwiać cykliczną identyfikację oprogramowania.</div> <div>12. Moduł musi posiadać funkcjonalność monitoringu rzeczywistego wykorzystania oprogramowania.</div> <div>13. Moduł musi umożliwiać zarządzanie zasobami oraz inwentaryzację systemowo-sprzętową.</div>	
Zarządzanie incydentami	<div>1. Moduł musi umożliwiać zarządzanie incydem i problemami użytkowników.</div> <div>2. Moduł musi umożliwiać użytkownikom zgłaszanie incydentów i problemów do działów technicznych.</div> <div>3. Moduł musi gromadzić całą historię prac i informować o postępie w realizacji zleceń.</div> <div>4. Moduł musi umożliwiać użytkownikom przeglądanie i przeszukiwanie własnych zgłoszeń.</div> <div>5. Moduł musi umożliwiać użytkownikowi korespondencję z opiekunami zgłoszeń.</div>	SPEŁNIA TAK /NIE
Monitoring użytkowników	<div>1. Moduł musi dostarczać informacje na temat aktywności pracowników w sieci.</div> <div>2. Moduł musi dostarczać informacji na temat aplikacji z których korzystają pracownicy.</div> <div>3. Moduł musi prezentować dane za pomocą przejrzystych zestawień i wykresów.</div> <div>4. Moduł musi posiadać system analizy wydruków.</div> <div>5. Moduł musi umożliwiać przegląd plików kopiowanych od/do stanowiska.</div> <div>6. Moduł musi umożliwiać blokadę portów USB, FDD, CD.</div> <div>7. Moduł musi umożliwiać autoryzację zewnętrznych nośników danych.</div> <div>8. Moduł musi umożliwiać podgląd urządzeń które były podłączane do konkretnych stanowisk.</div> <div>9. Moduł musi umożliwiać przeglądanie historii poszczególnych aplikacji dla danego stanowiska.</div> <div>10. Moduł musi umożliwiać tworzenie listy aplikacji dozwolonych dla użytkownika.</div>	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

	11. Moduł musi umożliwiać podgląd pełnej historii przeglądania stron WWW dla danego stanowiska. 12. Moduł musi umożliwiać tworzenie list stron WWW które mogą być „zabronione” lub „dozwolone” dla użytkownika. 13. Moduł musi umożliwiać informowanie o aktywnościach użytkowników, danych logowania do systemu, blokady lub uśpienia.	
Zdalne zarządzanie	1. Moduł musi umożliwiać zdalne zarządzanie komputerem. 2. Moduł musi umożliwiać zdalne połączenie między administratorem a komputerem użytkownika. 3. Moduł musi umożliwiać zdalny transfer plików. 4. Moduł musi posiadać możliwość wysyłania wiadomości do wybranych użytkowników lub komunikację za pomocą czatu tekstowego. 5. Moduł musi umożliwiać zdalną instalację oprogramowania. 6. Moduł musi umożliwiać centralne zarządzanie kopiami zapasowymi danych użytkowników.	SPEŁNIA TAK /NIE
Monitoring sieci	1. Moduł musi pozwalać na cykliczne skanowanie sieci LAN. 2. Moduł musi umożliwiać analizę wykrytych urządzeń. 3. Moduł musi dostarczać informację na temat stanu drukarek i urządzeń sieciowych. 4. Moduł musi analizować ruch sieciowy pomiędzy urządzeniami. 5. Moduł musi automatycznie informować o dostępności usług oraz awariach urządzeń. 6. Moduł musi umożliwiać konfigurację sieci przed procesem skanowania. 7. Moduł umożliwia tworzenie listy wykrytych urządzeń sieciowych.	SPEŁNIA TAK /NIE
Ilość	1 szt.	SPEŁNIA TAK /NIE

22. Usługi informatyczne: wdrożenie systemu monitorowania środowiska serwerowego

Nazwa	Minimalne wymagania dla usługi	
Typ	Wdrożenie systemu monitorowania środowiska serwerowego w Urzędzie Gminy - wdrożenie zdalne	SPEŁNIA TAK /NIE
Opis wdrożenia	1. Przygotowanie maszyny wirtualnej z preinstalowanym systemem 2. Wstępna konfiguracja oraz adresacja IP zgodnie z wymaganiami Zamawiającego. 3. Konfiguracja użytkowników systemu zgodnie z wymaganiami Zamawiającego. 4. Konfiguracja powiadomień e-mail.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

	5. Instalacja agentów systemu na wskazanych przez zamawiającego serwerach. 6. Podłączenie urządzeń wskazanych przez Zamawiającego zgodnych z dostępnymi szablonami systemu. 7. Przygotowanie dokumentacji powdrożeniowej.	
Ilość	1 szt.	SPEŁNIA TAK /NIE



**Opis przedmiotu zamówienia****II. OBSZAR KOMPETENCYJNY****1 SZKOLENIE DLA DZIAŁU IT (szkolenie dot. UTM).**

L.P	Nazwa	Minimalne wymagania dla szkolenia	Oferowane parametry
		Zamówienie będzie realizowane na rzecz <b>Urzędu Gminy Rogowo</b> .	
1.	Typ	Szkolenie z zakresu urządzenia klasy UTM wdrażanego w ramach projektu (Cześć I Obszar techniczny, pkt. 1. UTM Unified Threat Management: wznowienie supportu dla Urzędu Gminy w Rogowie oraz pkt. 2. UTM Unified Threat Management: urządzenie klasy UTM dla Ośrodka Pomocy Społecznej w Rogowie, 2 osoby formuła online.	SPEŁNIA TAK /NIE
2.	Czas trwania	Minimum 3 dni (1 dzień = 8 godzin roboczych 3 dni =24 godziny robocze)	SPEŁNIA TAK /NIE
3.	Lokalizacja	Szkolenie online	SPEŁNIA TAK /NIE
4.	Wymagany minimalny zakres tematyczny	<ul style="list-style-type: none"> <li>Architektura urządzeń producenta,</li> <li>Wirtualizacja w obrębie urządzenia</li> <li>Wstępna konfiguracja urządzenia,</li> <li>Zaawansowania konfiguracja sieci i routingu</li> <li>Uwierzytelnianie użytkowników</li> <li>Tworzenie reguł firewall w oparciu o grupy użytkowników</li> <li>Dwuskładnikowa autoryzacja</li> <li>Wirtualne sieci prywatne- VPN</li> <li>Diagnostyka i rozwiązywanie problemów</li> <li>Konfiguracja urządzeń do pracy w klastrze HA</li> </ul>	SPEŁNIA TAK /NIE
5.	Trenerzy	Certyfikowani przez producenta rozwiązania.	SPEŁNIA TAK /NIE
6.	Materiały szkoleniowe	Materiały elektroniczne	SPEŁNIA TAK /NIE
7.	Ilość	2 szt.	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia**2 SZKOLENIE DLA DZIAŁU IT (szkolenie Microsoft Active Directory)**

L.P	Parametr	Charakterystyka (wymagania minimalne) Oferowane parametry	Oferowane parametry
		Zamówienie będzie realizowane na rzecz <b>Urzędu Gminy Rogowo.</b>	
1.	Typ	Szkolenie dla działu IT dotyczące usługi katalogowej systemów Windows Server (Microsoft Active Directory) dla Urzędu Gminy w Rogowie dla 2 osób, formuła online.	SPEŁNIA TAK /NIE
2.	Czas trwania	Minimum 2 dni tj.: (1 dzień = 8 godzin roboczych 2 dni =16 godzin roboczych)	SPEŁNIA TAK /NIE
3.	Lokalizacja	Szkolenie online	SPEŁNIA TAK /NIE
4.	Wymagany minimalny zakres tematyczny	<p>Szkolenie musi zawierać co najmniej poniższe zagadnienia:</p> <ul style="list-style-type: none"> <li>• Instalacja i konfiguracja kontrolerów domeny <ul style="list-style-type: none"> <li>○ Omówienie usług Active Directory Domain Services</li> <li>○ Omówienie kontrolerów domeny usług AD DS</li> <li>○ Wdrożenie kontrolera domeny</li> <li>○ Omówienie usługi Encrypted DNS</li> </ul> </li> <li>• Zarządzanie obiektami w Active Directory Domain Services <ul style="list-style-type: none"> <li>○ Zarządzanie kontami użytkowników</li> <li>○ Zarządzanie grupami w usługach AD DS</li> <li>○ Zarządzanie obiektami typu komputer w AD DS</li> <li>○ Wdrażanie i zarządzanie jednostek organizacyjnych w AD DS</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

		<ul style="list-style-type: none"><li>• Zarządzanie zaawansowaną infrastrukturą Active Directory Domain Services<ul style="list-style-type: none"><li>◦ Wprowadzenie do zaawansowanych wdrożeń AD DS</li><li>◦ Wdrożenie rozproszonego środowiska AD DS</li><li>◦ Konfiguracja relacji zaufania AD DS.</li></ul></li><li>• Wdrażanie i zarządzanie lokacjami i repliką Active Directory Domain Services<ul style="list-style-type: none"><li>◦ Omówienie replikacji usług AD DS.</li><li>◦ Konfigurowanie lokacji usług AD DS.</li><li>◦ Konfigurowanie i monitorowanie replikacji usług AD DS.</li></ul></li><li>• Wdrażanie zasad grupy<ul style="list-style-type: none"><li>◦ Wprowadzenie do zasad grupy</li><li>◦ Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)</li><li>◦ Konfiguracja zakresu przetwarzania obiektów GPO</li><li>◦ Rozwiązywanie problemów GPO</li></ul></li><li>• Zarządzanie ustawieniami użytkowników za pomocą zasad grupy<ul style="list-style-type: none"><li>◦ Wdrażanie szablonów administracyjnych</li><li>◦ Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów</li><li>◦ Konfiguracja preferencji zasad grupowych</li></ul></li></ul>	
5.	Trenerzy	Trenerzy prowadzący szkolenie muszą posiadać certyfikat producenta rozwiązania.	SPEŁNIA TAK /NIE
6.	Materiały szkoleniowe	Materiały elektroniczne	SPEŁNIA TAK /NIE
7.	Wsparcie trenera po szkoleniu	Co najmniej 14 dni	SPEŁNIA TAK /NIE
8.	Ilość	2 szt.	SPEŁNIA TAK /NIE



**3 SZKOLENIE DLA PRACOWNIKÓW SPOZA DZIAŁU IT (cyberbezpieczeństwo).**

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
		Zamówienie będzie realizowane na rzecz <b>Urzędu Gminy Rogowo</b> .	
1.	Typ	Szkolenie dla pracowników spoza działu IT (cyberbezpieczeństwo)- szkolenie dla pracowników Urzędu Gminy (1 grupa, 30 osób, szkolenie online).	SPEŁNIA TAK /NIE
2.	Przygotowanie i przeprowadzenie kampanii phishingowej	<p>Zakres i planowany przebieg Testów phishingowych (TP) w zakresie minimum:</p> <ol style="list-style-type: none"> <li>1. Zamawiający wymaga ustalenia scenariusza w zakresie minimum: Opracowania i zatwierdzenie z Zamawiającym szczegółowego scenariusza ataku socjotechnicznego. Wyboru metod i narzędzi do jego realizacji. Szczegóły kampanii, w tym scenariusze socjotechniczne oraz harmonogram realizacji, muszą zostać ustalone i zatwierdzone przez Zamawiającego co najmniej 14 dni przed planowanym rozpoczęciem kampanii.</li> <li>2. Zamawiający wymaga przeprowadzenia przygotowań ataku w zakresie minimum: <ul style="list-style-type: none"> <li>• Projektowanie minimum 1 szablonu mailowych</li> <li>• Przygotowanie minimum 1 fałszywej domeny i konfiguracja hostingu.</li> <li>• Listy odbiorców</li> <li>• Finalizacja listy docelowych odbiorców w oparciu o informacje uzyskane od Zamawiającego.</li> </ul> </li> <li>3. Zamawiający wymaga przeprowadzenie startu realizacji ataku w zakresie minimum: <ul style="list-style-type: none"> <li>• Rozpoczęcie kampanii phishingowej:</li> <li>• Kampania musi zostać przeprowadzona w ciągu minimum 3 dni, rozpoczynając się od wysyłki mailowej do wybranych odbiorców.</li> </ul> </li> <li>4. Zamawiający wymaga kontynuacji kampanii i monitorowania w zakresie minimum:</li> </ol>	SPEŁNIA TAK /NIE

Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

		<ul style="list-style-type: none"><li>Dostosowania harmonogramu wysyłki do ustaleń przeprowadzonych z Zamawiającym na etapie ustalania scenariusza.</li><li>Czas trwania kampanii od min 3 dni roboczych zostaje dostosowana w oparciu o ustalenia z Zamawiającym przeprowadzone podczas pierwszego etapu – Ustalenie scenariusza.</li><li>Kampania powinna być realizowana etapami, z wysyłkami dokonywanymi w określonych partiach i godzinach, aby zapewnić maksymalną skuteczność.</li><li>Monitorowanie reakcji pracowników urzędu</li><li>Bieżące śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami</li><li>Analiza efektywności i w razie potrzeby, wprowadzanie zmian w strategii kampanii.</li></ul> <p>5. Zamawiający wymaga przeprowadzenia zakończenia kampanii i przygotowanie raportu w zakresie minimum:</p> <ul style="list-style-type: none"><li>Zakończenie wysyłki mailowej- przedstawienie efektów</li><li>Zebranie i dokonanie pierwszej analizy zebranych danych na temat interakcji i reakcji na przeprowadzone działania.</li><li>Przygotowania raportu końcowego dotyczącego skuteczności kampanii, zawierającego wszystkie zebrane dane, zakresie minimum:</li></ul> <p>A. Opis wykorzystanych i skonfigurowanych domen</p> <p>B. Opis szablonów oraz opis celu jaki stanowi podczas realizacji kampanii</p> <p>C. Opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku</p> <p>D. Statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane.</p> <p>E. Podsumowanie oraz rekomendacje</p>	
3.	Szkolenie z cyberbezpieczeństw a	<p>Szkolenie musi zostać przeprowadzone w jednej grupie liczącej maksymalnie 30 osób. Szkolenie online trwające minimum 1 godzinę. Szkolenie musi obejmować w zakresie minimum:</p> <ul style="list-style-type: none"><li>Wycieki informacji – mechanizmy i skutki.</li></ul>	SPEŁNIA TAK /NIE



Opis przedmiotu zamówienia

Fundusze Europejskie

na Rozwój Cyfrowy

		<ul style="list-style-type: none"><li>• Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze.</li><li>• Psychomanipulacja w sieci – zasady i zastosowania.</li><li>• Sfałszowane komunikaty i strony – identyfikacja zagrożeń.</li><li>• Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing)</li><li>• Archiwizacja internetowa – cyfrowy ślad nie znika.</li><li>• Mechanizmy śledzenia w sieci – rola i funkcja cookies.</li><li>• Niebezpieczeństwa ze strony nieautoryzowanego sprzętu.</li><li>• Ataki siłowe na hasła – jak nie dać się złamać.</li><li>• Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing).</li><li>• Świadomość pracowników – kultura bezpieczeństwa w organizacji.</li></ul>	
4.	Ilość	1 szt.	SPEŁNIA TAK /NIE

