Załącznik nr 10 do SWZ

**Opis Przedmiotu Zamówienia**

Projekt pn. „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Gminy w Lubszy”, realizowany w ramach Grantu Fundusze Europejskie na Rozwój Cyfrowy (FERC), II Zaawansowane Usługi Cyfrowe, 2.2 Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa, nr naboru FERC.02,02-CS.01-001/23

Lubsza, styczeń 2026

Spis treści

[Wstęp 3](#_Toc217308117)

[Ogólne zasady równoważności rozwiązań 4](#_Toc217308118)

[Wymagania ogólne 7](#_Toc217308119)

[Harmonogram realizacji przedmiotu zamówienia 8](#_Toc217308120)

[Dostawa sprzętu 9](#_Toc217308121)

[Serwer do klastra wysokiej dostępności – 2 sztuki 9](#_Toc217308122)

[UTM 11](#_Toc217308123)

[Macierz do kopii zapasowych 29](#_Toc217308124)

[Dysk sieciowy NAS 48](#_Toc217308125)

[Zasilacz awaryjny do szafy RACK – 3 sztuki 50](#_Toc217308126)

[Zasilacz awaryjny dla stacji roboczych – 16 sztuk 52](#_Toc217308127)

[Switch do szafy RACK – 2 sztuki 53](#_Toc217308128)

[Dostawa oprogramowania 55](#_Toc217308129)

[Oprogramowanie do monitoringu zasobów IT 55](#_Toc217308130)

[System klasy SIEM 57](#_Toc217308131)

[Udzielenie dostępu do platformy szkoleniowej on-line 63](#_Toc217308132)

[Oprogramowanie do inwentaryzacji i zarządzania 72](#_Toc217308133)

[Wdrożenie i konfiguracja elementów bezpieczeństwa 75](#_Toc217308134)

[Oprogramowanie do monitoringu zasobów IT 75](#_Toc217308135)

[System klasy SIEM 75](#_Toc217308136)

[Platforma szkoleniowa 76](#_Toc217308137)

[Opracowanie SZBI oraz akttualizacja PBI dla Urzędy oraz 5 jednostek podległych 77](#_Toc217308138)

# Wstęp

Niniejszy dokument stanowi Opis Przedmiotu Zamówienia w zakresie dostawy, instalacji i konfiguracji sprzętu oraz dostawy licencji i wdrożenia oprogramowania zwiększającego poziom bezpieczeństwa cybernetycznego w Urzędzie Gminy w Lubszy.

Ramowy zakres projektu to:

* dostawa i konfiguracja sprzętu,
* dostawa licencji i konfiguracja zaawansowanych systemów bezpieczeństwa,
* dostawa, instalacja i konfiguracja platformy szkoleniowej,
* świadczenie usługi serwisowej, aktualizacji oprogramowania do najnowszych wersji i wsparcia na okres 7 miesięcy, ale nie dłużej niż do 30.06.2026r.

# Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający, zgodnie z ustawą Prawo zamówień publicznych, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy (poza wyjątkami gdzie nie ma możliwości zastosowania rozwiązań równoważnych). Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.

# Wymagania ogólne

Zamawiający wymaga, aby sprzęt będący przedmiotem dostawy był wyprodukowany nie wcześniej niż 12 miesięcy od dnia dostawy. Oprogramowanie musi być dostarczone i zainstalowane w wersji aktualnej (stabilnej) na dzień jego instalacji.

W ramach prowadzonych prac, a w szczególności prac konfiguracyjnych, Zamawiający oczekuje utrzymania funkcjonalności wszystkich posiadanych przez siebie systemów i aplikacji. Prace wdrożeniowe muszą być przeprowadzone w taki sposób, aby nie zakłócić normalnej pracy urzędu. Jeżeli podczas prowadzonych prac zaistnieje konieczność rekonfiguracji posiadanych przez Zamawiającego systemów, Wykonawca jest zobowiązany dokonać takich rekonfiguracji na własną odpowiedzialność oraz własny koszt.

Zamawiający oczekuje, aby wszystkie wdrożone usługi były zgodne z ITIL (Information Technology Infrastructure Library) w zakresie najlepszych praktyk zarządzania usługami IT w celu zwiększenia efektywności, skuteczności oraz bezpieczeństwa operacji IT, w szczególności w efektywnym zarządzaniu ryzykiem, reagowaniu na incydenty bezpieczeństwa, a także w zapewnieniu zgodności z przepisami prawnymi i standardami branżowymi.

# Harmonogram realizacji przedmiotu zamówienia

Harmonogram rzeczowo-finansowy z podziałem na etapy wraz z wartością, kolejność realizacji zakresów, kamienie milowe zostanie ustalony opracowany przez Wykonawcę w porozumieniu z Zamawiającym i zaakceptowany przez Zamawiającego w ciągu 7 dni od daty podpisania Umowy.

# Dostawa sprzętu

## Serwer do klastra wysokiej dostępności – 2 sztuki

|  |  |
| --- | --- |
| Cecha | Wymaganie minimalne |
| Ogólne | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |
| Obudowa | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |
| Procesor | Architektura x86, maksymalny TDP dla procesora – 120W. Minimalna ilość rdzeni dla pojedynczego procesora – 12, zegar min 2.8GHz. Wsparcie dla procesorów do 24 rdzeni. |
| Liczba procesorów | 2 |
| Płyta główna | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon). |
| Pamięć operacyjna | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 3200MHz . Minimum 16 slotów na pamięć. Możliwość rozbudowy do 1TB RAM. |
| Zabezpieczenie pamięci | Memory registred ECC |
| Rozbudowa dysków | W chwili dostawy każdy serwer musi posiadać zainstalowane minimum 2 dyski o pojemności nie mniejszej niż 960GB M.2 oraz 2 dyski 8TB HDD. |
| Zasilanie | Minimum dwa redundantne zasilacze. |
| Interfejsy sieciowe | Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  Karta SFP+ 2 Porty nie zajmująca portu PCIe  Cztery porty 1Gb baseT |
| Dodatkowe sloty I/O | Obudowa z obsługą min. 3 slotów PCIe |
| Dodatkowe porty | 2x USB 2.0 ,1x USB 3.0, VGA port |
| Zarządzanie | Możliwość zdalnego zarządzania serwerem, udostępniania zdalnej konsoli graficznej i podłączania zdalnych napędów. |
| Funkcje zabezpieczeń | Hasło włączania, hasło administratora, moduł TPM (wspierający TPM 2.0) |
| System operacyjny | Windows Server 2025 Standard oraz 50 licencji dostępowych typu User CAL (dla całego klastra) |
| Gwarancja (minimalnie) | 36 miesięcy gwarancji producenta. Serwis świadczony bezpośrednio przez producenta sprzętu. W przypadku awarii dysków uszkodzone nośniki pozostają u Zamawiającego. |

## UTM

|  |  |
| --- | --- |
| Cecha | Wymaganie minimalne |
| Ogólne | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. |
| System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. |
| System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. |
| Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
| Monitoring stanu realizowanych połączeń VPN. |
| System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie | System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:   * 7 portami Gigabit Ethernet RJ-45. |
| System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. |
| System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. |
| System jest wyposażony w zasilanie AC. |
| Parametry wydajnościowe | W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. |
| Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. |
| Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. |
| Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. |
| Funkcje Systemu Bezpieczeństwa | W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |
| System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. |
| W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. |
| Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. |
| Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. |
| Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.   * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| Połączenia VPN | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. |
|  | System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. |
| SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
| System daje możliwość określania pasma dla poszczególnych aplikacji. |
| System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. |
| System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
| Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. |
| System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. |
| System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. |
| System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. |
| System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
| System chroni przed atakami na aplikacje pracujące na niestandardowych portach. |
| Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
| System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |
| Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). |
| Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. |
| Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
| Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
| Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |
| Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |
| Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. |
| Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). |
| System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |
| W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |
| Filtr WWW dostarcza kategorii stron zabronionych prawem np.: hazard. |
| Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |
| Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). |
| Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. |
| Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. |
| Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. |
| System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.   Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. |
| System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. |
| 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. |
| Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http. |
| Zarządzanie | 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. |
| Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. |
| Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |
| System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. |
| System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
| Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). |
| Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |
| W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |
| Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. |
| Możliwość włączenia logowania per reguła w polityce firewall. |
| System zapewnia możliwość logowania do serwera SYSLOG. |
| Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Tokeny sprzętowe | System musi wspierać możliwość dodatkowego składnika autorazacji dla użytkowników usługi VPN. Zamawiający wymaga dostawę 10 szt tokenów sprzętowych kompatybilnych z urządzeniem i pracujących w standardzie OATH HOTP. |
| Certyfikaty | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. |
| Gwarancja oraz wsparcie | System jest objęty serwisem gwarancyjnym producenta przez okres min. 24 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. |
| 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 do dnia 30.05.2026 r.. |

## Macierz do kopii zapasowych

|  |  |
| --- | --- |
| Cecha | Wymaganie minimalne |
| Zarządzanie i magazyny | 1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. 2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu. 3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:    1. Obudowa rack rozmiar: 1U    2. Procesor: min. 8 rdzeni, 16 wątków, częstotliwość bazowa 2.60 GHz w architekturze x86-64    3. Pamięć RAM: minimum 16 GB    4. Przestrzeń dostępna na przechowywanie danych: Min. 26 TB po RAID 5    5. Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,    6. Redundantne zasilanie,    7. Interfejsy sieciowe: Min. 2szt. Ethernet 1Gb, SFP+    8. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania. 4. Produkt dostępny w polskiej wersji językowej. 5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej 6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków 7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów 8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych 9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT 10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft 11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe 12. System zarządzania nie może być oparty o relacyjne bazy danych. 13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej). 14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). 15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych. 16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych. 17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. 18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. 19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej. 20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie. 21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. 22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. 23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych 24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS. 25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego. 26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii). 27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane. 28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione. 29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika, 30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta. 31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym. 32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych). 33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych. 34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów. 35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych 36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie. 37. Proces deduplikacji realizowany jest blokiem o zmiennej wielkości. Wielkość ta ustalona jest dynamicznie w trakcie wykonywania kopii zapasowej w celu zapewnienia jak najwyższej efektywności procesu. 38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego. 39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki. 40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu. 41. System musi pozwalać na automatyczne aktualizacje oprogramowania. 42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS. 43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia. 44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji. 45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany. 46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane. 47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników. 48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych. 49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów. 50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania. 51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego. 52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych. 53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental, 55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC). 56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance’u 57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny 58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS). 59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu. 60. Możliwość generowania raportów dobowych w oparciu o harmonogram 61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski) 62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna) 63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP. 64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu). |
| Środowiska fizyczne i bazy danych | 1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. 2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. 4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption. 5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji. 6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych. 7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. 8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. 9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. 11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. 12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). 13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych. 14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows). |
| Środowiska wirtualne | 1. System musi posiadać wsparcie dla wirtualizatorów VMware vSphere, Microsoft Hyper-V 2. Dla wspieranych wirtualizatorów system musi posiadać możliwość zabezpieczania całych maszyn wirtualnych bez konieczności instalacji agentów backupowych wewnątrz maszyn wirtualnych 3. Dla wspieranych środowisk wirtualnych system musi umożliwiać wykonanie kopii pełnej, różnicowej oraz przyrostowej, a dodatkowo umożliwiać wykonanie procesu deduplikacji 4. System musi wspierać kopię w trybie application-aware dla wirtualizatorów Hyper-V oraz vSphere. 5. Dla środowiska VMware, system musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych. 6. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. 7. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner. 8. Dla wybranych wirtualizatorów, system kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. 9. Rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). 10. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku dla wybranych wirtualizatorów. |
| Licencjonowanie i wsparcie techniczne | 1. Wszystkie linie supportu muszą być obsługiwane w języku polskim. 2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta. 3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu. 4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów) 5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego. 6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego. 7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera. 8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych. 9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu. 10. Wsparcie techniczne producenta musi zostać dostarczone na okres do 30.06.2026r. |
| Antyransomware i bezpieczeństwo | 1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików"). 2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System 3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty. 4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii. 5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu. |

## Dysk sieciowy NAS

|  |  |
| --- | --- |
| Parametr | Wymagania minimalne |
| Ogólne | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |
| Obudowa | RACK |
| Kieszenie na dyski | 4 szt 2,5”/3,5” hot swap |
| Zainstalowane dyski | 4 szt. 3,5” 8TB |
| Pamięć RAM | 8 GB z możliwością rozbudowy |
| RAID | 0, 1, 5, 6, 10 |
| Procesor | 4 rdzenie, 2.0 GHz w architekturze x86 |
| Protokoły sieciowe | AFP  Dynamiczny DNS (DDNS)  HTTP  HTTPS  iPv4/iPv6  iSCSI  Klient DHCP lub statyczny adres IP  Klient VPN  Obsługa ramek typu jumbo  Serwer CIFS/SMB  Serwer DHCP  Serwer FTP  Serwer SFTP  NFS  SNMP  SSH  Telnet  VLAN (802.1Q)  Wake-On-LAN  TFTP  WebDAV  LDAP |
| System plików | EXT4 |
| System plików dla dysków zewnętrznych | FAT32  exFAT  NTFS  HFS+  EXT3  EXT4 |
| Gwarancja | 36 miesięcy na urządzenie oraz dyski |

## Zasilacz awaryjny do szafy RACK – 3 sztuki

|  |  |
| --- | --- |
| Parametr | Wymagania minimalne |
| Ogólne | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |
| Moc znamionowa | Min. 2700W |
| Obudowa | Do montażu w szafie Rack 19” |
| Maksymalna wysokość UPS | Maks. 4U (bez dodatkowych modułów bateryjnych) |
| Maksymalna głębokość | Maks. 800 mm |
| Zakres napięcia wejściowego | Min. 110-290V |
| Napięcie nominalne wyjściowe | 200/208/220/230/240V AC |
| Gniazda wyjściowe | 6x IEC320 C13-10A |
| Częstotliwość wyjściowa | 45-65Hz (wykrywana automatycznie) |
| Czas podtrzymania dla obciążenia 100% | Min. 3-5 minut |
| Interfejs użytkownika | Wyświetlacz LCD |
| Gwarancja na akumulatory | Min. 24 miesiące |

## Zasilacz awaryjny dla stacji roboczych – 16 sztuk

|  |  |
| --- | --- |
| Parametr | Wymagania minimalne |
| Ogólne | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |
| Topologia | Line-interactive |
| Obudowa | Tower |
| Moc pozorna | 1200 VA |
| Moc skuteczna | 650 W |
| Napięcie wejściowe | 140-300 V |
| Gniazda wyjściowe | IEC 320 C13 – 6szt. |
| Czas przełączania | 6 ms |
| Czas podtrzymania dla obciążenia 50% | 4 min |
| Zabezpieczenia | Przeciwzwarciowe  Przeciążeniowe  Przeciwprzepięciowe |
| Gwarancja | 24 miesiące |

## Switch do szafy RACK – 2 sztuki

|  |  |
| --- | --- |
| **Obudowa** | RACK |
| **Ogólne** | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |
| **Typ przełącznika** | Zarządzalny |
| **Przełącznik wielowarstwowy** | L2 |
| **Liczba portów** | 48x Gigabit Ethernet (10/100/1000)  4x SFP+ |
| **Przepustowość przełączania** | Min. 170 GBit/s |
| **Przepustowość** | Min. 250 Mpps |
| **Wielkość tabeli adresów** | 32000 wejścia |
| **Pamięc bufora pakietów** | 2 MB |
| **Wielkość pamięci flash** | 64 MB |
| **Pojemność i typ pamięci wewnętrznej** | 512 MB DDR3-SDRAM |
| **Dodatkowe funkcje** | Obsługa 10G  Agregator połączenia  Obsługa VLAN  Protokół drzewa rozpinającego |
| **Interoperacyjność** | Urządzenie musi być zarządzane ze wspólnej konsoli (co najmniej interfejs www) z dostarczanym urządzeniem UTM |
| **Gwarancja** | Minimum 24 miesiące |

# Dostawa oprogramowania

## Oprogramowanie do monitoringu zasobów IT

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Głównym zadaniem do realizacji przez system monitoringu jest zarządzanie wydajnością i dostępnością w zakresie komponentów tj.: - serwery - urządzenia sieciowe - bazy danych - aplikacje System musi wspomagać administrowaniu w proaktywnym zarządzaniu kondycją infrastruktury IT identyfikując potencjalne problemy i awarie, zanim wpłyną one negatywnie na działanie Urzędu. |
| System musi umożliwiać monitorowanie urządzeń zarówno w sposób agentowy jak i bezagentowy (sieciowy) |
| System musi umożliwiać monitorowanie agentowe co najmniej systemów: - Microsoft Windows - Linux (dowolna dystrybucja) - MacOS |
| System musi posiadać możliwość monitorowanie bezagentowego dostępności i wydajności dowolnej witryny WWW |
| System musi umożliwiać bezagentowy monitoring z wykorzystaniem protokołów SNMP |
| System musi być dostarczony na licencji umożliwiającej na monitorowanie dowolnej liczby komponentów IT i pracę dowolnej liczby operatorów |
| System musi posiadać narzędzia do zbierania danych o wydajności i dostępności usług |
| System musi umożliwiać konfigurację interwałów i częstotliwości monitoringu poszczególnych komponentów lub grup komponentów |
| System musi posiadać narzędzia umożliwiające wizualizację danych w postaci wykresów |
| System musi umożliwiać budowanie map infrastruktury sieci oraz osadzania komponentów na mapach |
| System musi posiadać mechanizm alertów z możliwością ich wysyłki co najmniej przez email, sms, MS Teams |
| System musi posiadać API umożliwiającego integrację z innymi narzędziami |
| System musi posiadać funkcję wykrywania anomalii oraz monitorowania trendów |
| System musi posiadać możliwość definiowania i zamawiania okresowych raportów dotyczących kondycji środowiska |
| System musi posiadać mechanizm budowania dedykowanych kokpitów do monitoringu |
| Komunikacja pomiędzy wszystkimi komponentami systemu musi odbywać się z wykorzystaniem bezpiecznych i szyfrowanych połączeń |
| System musi posiadać rozbudowany moduł zarządzania użytkownikami, grupami użytkowników oraz uprawnieniami |
| System musi umożliwiać uwierzytelnianie użytkowników przy pomocy: - kont wbudowanych - usługi katalogowej LDAP/AD - usługi pojedynczego logowania SSO |
| System musi posiadać narzędzia do automatycznego wykrywania i podłączania komponentów |

## System klasy SIEM

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Serwer | System musi być rozwiązaniem klasy SIEM z rozszerzeniem XDR umożliwiającym monitorowanie bezpieczeństwa, wykrywania zagrożeń, monitorowania integralności oraz odpowiedzi na incydenty. |
| System musi umożliwiać monitorowanie infrastruktury IT w czasie rzeczywistym. Infrastruktura IT Zamawiającego składa się z:   * 4 serwery * 1 urządzenie UTM * 2 przełączniki sieciowe |
| Komponenty serwerowe systemu muszą być możliwe do zainstalowania na systemie operacyjnym z rodziny Linux. |
| System musi być możliwy do zainstalowania w środowisku wirtualizacyjnym opartym o Proxmox VE. |
| Instalacja i konfiguracja systemu musi być możliwa do automatyzacji z wykorzystaniem Ansible. |
| Wykonawca w ramach zamówienia dostarczy wszelkie niezbędne licencje umożliwiające uruchomienie Systemu takie jak np. systemy operacyjne, serwery baz danych, itp. |
| System musi być dostarczony w konfiguracji wysokodostępnej (klaster High Availability) dla każdego z komponentów z wyłączeniem agentów. |
| System musi umożliwiać monitorowanie agentowe oraz bezagentowe (sieciowe). |
| Silnik system musi udostępniać API w technologii REST pozwalające na rejestrację zdarzeń, zarządzanie konfiguracją agentów oraz odczyt stanu każdego z monitorowanych komponentów. |
| Logowanie operatorów do systemu musi odbywać się z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością (SSO) co najmniej w zakresie protokołu SAML2. |
| System musi posiadać kontrolę dostępu opartą na rolach (RBAC). |
| System musi posiadać funkcję wysyłania powiadomień do użytkowników lub grup w odpowiedzi na występujące zagrożenia. System musi wysyłać powiadomienia co najmniej za pomocą email oraz SMS. |
| System musi być dostarczony wraz z wbudowanymi regułami detekcji. Musi istnieć możliwość dodawania własnych reguł. |
| System musi umożliwiać zaawansowane metody detekcji poprzez integrację z frameworkiem MITRE ATT&CK. |
| System musi wykrywać i aktywnie blokować ataki typu brute-force na hasła systemów operacyjnych. |
| System musi umożliwiać integrację z oprogramowaniem NIDS tj. Suricata. |
| System musi wykrywać i zapobiegać atakom typu SQL Injection. |
| System musi wykrywać i blokować ataki typu DDoS. |
| System musi umożliwiać wykrywania i usuwanie malware poprzez integrację z zewnętrznymi bazami i narzędziami tj. VirusTotal. |
| System musi wykrywać znane podatności na każdym monitorowanym obiekcie z wykorzystaniem baz CVE. |
| System musi wykrywać ukryte procesy oraz wykonywanie podejrzanych operacji przez zainstalowane w systemie operacyjnym monitorowanego obiektu aplikacje. |
| Agent | System musi udostępniać dedykowane pliki instalacyjne agentów dla systemów co najmniej Windows, Linux oraz MacOS. |
| Agent musi komunikować się z serwerem systemu za pomocą szyfrowanego i autoryzowanego połączenia. |
| Agent musi posiadać funkcjonalność zdalnej konfiguracji oraz zdalnej aktualizacji po podłączeniu się do serwera. |
| Agent musi posiadać budowę modułową z możliwością wyłączenia poszczególnych modułów w zależności od wymaganej konfiguracji oraz możliwości wydajnościowych monitorowanego obiektu. |
| Agent musi posiadać co najmniej następujące moduły:   * Moduł zbierania logów (kolektor logów) * Moduł wykonywania poleceń * Moduł monitorowania integralności plików * Moduł inwentaryzacji zasobów * Moduł oceny konfiguracji bezpieczeństwa (SCA) * Moduł wykrywania podatności * Moduł zgodności ze standardami bezpieczeństwa * Moduł reaktywnej odpowiedzi * Moduł wykrywania malware |
| Agent musi posiadać kolektor logów wspierający filtry XPath do przetwarzania Dziennika zdarzeń systemu Windows. |
| Kolektor logów musi wspierać odczyt wielolinijkowych logów (co najmniej format Linux Audit). |
| Monitor integralności plików musi umożliwiać rejestrowania zdarzeń tj. utworzenie pliku, modyfikacja lub usunięcie wraz ze wskazaniem użytkownika oraz czasu zdarzenia. Dodatkowo moduł musi umożliwiać monitorowanie zmian atrybutów, uprawnień, właściciela oraz monitoring zawartości pliku. |
| Moduł inwentaryzacji zasobów musi zbierać i udostępniać informacje o obiekcie w zakresie co najmniej:   * Rodzaj i wersja systemu operacyjnego, * Lista i rodzaj interfejsów sieciowych, * Lista aktywnych procesów systemu operacyjnego, * Lista zainstalowanych aplikacji, * Lista otwartych portów sieciowych. |
| Moduł oceny konfiguracji bezpieczeństwa musi umożliwiać, za pomocą predefiniowanych reguł, skanowanie obiektu w celu wykrycia zagrożeń lub błędnych konfiguracji w zakresie co najmniej:   * Siła haseł, * Usunięcie niepotrzebnego lub niebezpiecznego oprogramowania, * Wyłączenie zbędnych usług   Moduł musi posiadać predefiniowane reguły SCA dla każdego z wymaganych systemów operacyjnych oraz udostępniać możliwość tworzenia własnych polityk SCA. |
| Moduł wykrywania podatności musi umożliwiać wykrywania luk w aplikacjach zainstalowanych na obiekcie za pomocą dostawców tj. National Vulnerability Database, Red Hat, Canonical, ALAS, MSU. |
| Moduł zgodności ze standardami bezpieczeństwa musi umożliwiać badania obiektu pod katem zgodności ze standardami tj. PCI DSS, HIPAA, NIST 800-53 oraz GDPR. |
| Moduł reaktywnej odpowiedzi musi umożliwiać automatyczne (bez udziału operatora SIEM) uruchomienie akcji tj.:   * Zablokowanie połączenia sieciowego, * Zatrzymanie aktywnego procesu, * Usunięcie pliku, * Przeskanowanie pliku pod kątem obecności wirusów. |
| Moduł wykrywania malware musi posiadać możliwość wykrywania anomalii i na tej podstawie obecności złośliwego oprogramowania. Moduł musi umożliwiać wykrywania ukrytych procesów, ukrytych plików oraz podejrzanych otwartych portów TCP/UDP. |

## Udzielenie dostępu do platformy szkoleniowej

Zamawiający wymaga przygotowania i udostępnienia w infrastrukturze własnej, bądź chmurowej platformy szkoleniowej zawierającej kursy dotyczące cyberbezpieczeństwa. Platforma musi być dostępna bez ograniczenia liczby użytkowników dla wskazanych przez Zamawiającego kont na okres do 30.06.2026r. Platforma musi spełniać wymagania zestawione w poniższej tabeli.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | System musi umożliwiać kompleksowe przeprowadzanie szkoleń przez Internet. |
| System musi zapewniać instruktaże krok po kroku. |
| System musi umożliwiać dodanie filmów szkoleniowych. |
| System udostępniania poradniki i materiały dla uczestnika. |
| System umożliwia dodanie dwóch rodzajów uczestników szkoleń – urzędnik i mieszkaniec. |
| System musi umożliwiać przeszukiwanie bazy szkoleń. |
| System musi zapewniać możliwość wystawiania certyfikatów z odbytych szkoleń. |
| System generuje raporty pozwalające na kontrolę stopnia wykorzystania narzędzia. |
| System zbudowana jest w sposób modułowy i opiera się o architekturę klient-serwer: a) serwer (WWW/Aplikacji LMS/Bazy Danych), b) klient (dowolny system operacyjny, dowolna przeglądarka internetowa); |
| System musi zapewniać prowadzenie szkoleń za pośrednictwem Internetu z wykorzystaniem: a) komputerów, b) smartfonów, c) tabletów; |
| System umożliwia dostęp on-line do szkoleń z dowolnego systemu operacyjnego i dowolnej przeglądarki internetowej. |
| System musi umożliwiać prowadzenie szkoleń z wykorzystaniem kursów multimedialnych, książek elektronicznych, elementów audio/wideo, telewizji internetowej. |
| System jest wyposażony w platformę do zarządzania szkoleniami (LMS). |
| System posiada narzędzie dla autorów szkoleń do tworzenia kursów e-learning (LCMS). |
| System pozwala na modyfikację istniejących szkoleń (edycja m.in. w zakresie opisu kursów i zawartości). |
| System posiada mechanizm określenia dostępności szkoleń (w tym: czas dostępności, sposób zapisu, klucz dostępu, widoczność elementów, itp.). |
| System pozwala na dezaktywację szkoleń. |
| System udostępnia uprawnionym użytkownikom narzędzia do sprawdzania wiedzy i umiejętności opanowanych przez kursantów/uczniów z możliwością tworzenia bazy pytań kontrolnych różnego rodzaju spośród których tworzony jest test, w tym: jednokrotnego/wielokrotnego wyboru, prawda/fałsz, wartość liczbowa, odpowiedź tekstowa, itp. |
| System udostępnia narzędzia monitorowania i oceniania aktywności uczestników kursów z możliwością przypisywania oceny do zadań wykonanych przez kursantów. |
| System posiada mechanizm dziennika zawierającego wyniki przeprowadzanych testów/sprawdzianów. |
| Zarządzanie szkoleniami | System posiada interfejs oraz mechanizm pomocy kontekstowej w języku polskim. |
| System musi zapewniać nieograniczoną liczbę użytkowników |
| System musi zapewniać moduł raportowania. |
| System musi zapewniać współpracę z bazami danych. |
| System musi zapewniać zarządzanie programami i planowaniem szkoleń. |
| System musi zapewniać zarządzanie profilami/kontami użytkowników. |
| System musi zapewniać przypisywanie użytkownikom globalnie (w obrębie całego systemu) określonych ról (np. edytor, autor, administrator, itd.) lub lokalnie (w ramach pojedynczego kursu) wskazywanie uczestników kursu. |
| System musi zapewniać harmonogram kursu. |
| System musi zapewniać mechanizm administracji szkoleniami i kursantami. |
| System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami. |
| System musi zapewniać interfejs w języku polskim. |
| Tworzenie kursów | System musi zapewniać mechanizm pomocy kontekstowej w języku polskim. |
| System musi zapewniać dokumentację w języku polskim. |
| System musi zapewniać tworzenie scenariuszy lekcji. |
| System musi zapewniać możliwość umieszczania na stronach różnego rodzaju interakcji. |
| System musi zapewniać możliwość tworzenia kursów on-line. |
| System musi zapewniać tworzenie testów. |
| System musi zapewniać zarządzanie zawartością szkoleń. |
| System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami. |
| System musi zapewniać możliwość eksportu do LMS. |
| System musi zapewniać możliwość edycji wyglądu kursów. |
| System musi zapewniać interfejs w języku polskim. |
| System musi zapewniać mechanizm pomocy kontekstowej w języku polskim. |
| System musi zapewniać dokumentację w języku polskim. |
| Egzaminy | System musi umożliwić tworzenie egzaminów z kursu |
| System musi umożliwić dodanie więcej niż jednego egzaminu do kursu. |
| Tworzenie pytań do egzaminów powinno być możliwe do wykonania z dwóch miejsc: - z panelu administracyjnego  - z poziomu danego egzaminu.  Przy czym wszystkie pytania utworzone z poziomu egzaminu również trafiają na listę wszystkich pytań. |
| Tworzenie pytania powinno polegać na określeniu: - treści pytania - dodatkowego opisu - typu pytania - prawidłowej odpowiedzi - treści widomości dla poprawnej odpowiedzi - treści widomości dla niepoprawnej odpowiedzi - ilość punktów za prawidłową odpowiedź - wskazówki do odpowiedzi |
| System musi umożliwić korzystanie przynajmniej z poniższych typów pytań: - Jednokrotny wybór - jedna prawidłowa odpowiedź - Wielokrotny wybór - wiele prawidłowych odpowiedzi - Pytanie otwarte - należy wpisać odpowiedź - Sortowanie - ułożenie obiektów w prawidłowej kolejności - Sortowanie w macierzy - dopasowywanie elementów do siebie w tabeli dwuwymiarowej - Wypełnij puste miejsce - wypełnienie pustego miejsca znakiem, liczbą lub tekstem - Ocena - wskazanie wartości - Esej / Otwarta odpowiedź - dłuższa wypowiedź pisemna |
| W przypadku pytania: - Wielokrotny wybór - Pytanie otwarte - Sortowanie - Sortowanie w macierzy - Wypełnij puste miejsce w systemie musi istnieć możliwość określenia przyznanych punktów za każdą odpowiedź. |
| W przypadku pytania typu "Esej/Otwarta odpowiedź" musi istnieć możliwość wpisania odpowiedzi bezpośrednio w systemie oraz załączenia pliku. |
| System musi umożliwić przypisanie każdego pytania do jednego testu. |
| System musi umożliwić zapis każdego pytania jako szkic lub opublikować. |
| System musi umożliwić usunięcie każdego pytania lub przeniesienie do kosza oraz opublikowanie w dowolnym momencie. |
| System musi umożliwić eksport egzaminów do pliku xml |
| System musi umożliwić tworzenie nowego egzaminu poprzez: - manualne wprowadzenie - sklonowanie egzaminu który już istnieje w systemie - import z pliku xml |
| W przypadku tworzenie egzaminu manualnie należy wpisać tytuł strony, dodać treść (opcjonalnie) oraz wskazać pytania do egzaminu. |
| Wskazanie pytań do egzaminu musi odbywać się poprzez wskazanie pytań z repozytorium lub poprzez utworzenie ich z poziomu budowania testu. |
| System musi umożliwić przypisanie egzaminu do kursu |
| System musi umożliwić przypisanie egzaminu do konkretnej lekcji kursu |
| System musi umożliwić określenie od kiedy egzamin jest dostępny dla użytkowników: - natychmiast - test jest dostępny od momentu zapisania się na kurs - na podstawie daty zapisu - test dostępny X dni po zapisaniu się na kurs - konkretna data - test dostępny w konkretnym dniu, od określonej godziny |
|  | System musi umożliwić określenie czy wzięcie udziału w egzaminie wymaga ukończenia wcześniej innego egzaminu. Jeśli tak, należy wskazać jakie konkretnie egzaminy musi zdać użytkownik aby móc przystąpić do tego. |
|  | System musi umożliwić określenie procentowej ilosć punktów niezbędną do zdania egzaminu. |
|  | System musi umożliwić wskazanie szablonu dla wydawanego certyfikatu po zdanym egzaminie. |
|  | W systemie musi istnieć możliwość uruchomienia zapisywania egzaminu na serwerze |
|  | W systemie musi istnieć możliwość ograniczenia ilości podejść do egzaminu |
|  | Musi istnieć możliwość wymuszenia uzupełnienia wszystkich pytań w celu zakończenia egzaminu |
|  | Musi istnieć możliwość określenia limitu czasu na przesłanie egzaminu |
|  | Musi istnieć możliwość dodania materiałów dotyczących egzaminu (np. Materiałów edukacyjnych). |
|  | Musi istnieć możliwość uruchomienia egzaminu automatycznie lub po wybraniu startu przez egzaminowanego. |
|  | Musi istnieć możliwość przeglądu tabeli wszystkich pytań z możliwością podglądu podsumowania oraz pominięciem pytania |
|  | Musi istnieć możliwość ustawienia losowej kolejności pytań dla każdego uzytkownika |
|  | Musi istnieć możliwość określenia kilku wiadomości na zakończenie egzaminu (w zależności od osiągniętej ilości punktów). |
|  | Musi istnieć możliwość wyświetlenia użytkownikowi ilości zdobytych punktów oraz czasu poświęconego na egzamin. |
|  | System musi wysyłać powiadomienia do użytkownika o odbytym egzaminie |
|  | System musi wysyłać powiadomienia administratorowi o użytkownikach którzy odbyli egzamin |
|  | Musi istnieć możliwość ograniczenia czasu trwania egzaminu. W przypadku przekroczenia czasu przez użytkownika egzaminu zostaje zakończony administracyjnie. |
|  | System musi umożliwiać tworzenie certyfikatów ukończenia egzaminu |
|  | Tworzenie certyfikatu musi się odbywać za pomocą edytora blokowego. |
|  | System musi umożliwić użycie jednego certyfikatu do wielu egzaminów oraz tworeznie certyfikatów dla każdego egzaminu osobno. |
|  | System musi umożliwić przeglądanie statystyk egzaminu. |
|  | Statystyka z egzaminu musi zawierać przynajmniej informacje: - użytkownik egzaminowany - liczba punktów - ilość poprawnych odpowiedzi - ilosć niepoprawnych odpowiedzi - ilość użytych wskazówek - czas poświęcony na egzamin - wynik egzaminu |
|  | System musi umożliwić eksport pełnych statystyk z systemu do pliku CSV |

## Oprogramowanie do inwentaryzacji i zarządzania

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Inwentaryzacja IT | 1. Inwentaryzacja stacjonarnych i przenośnych komputerów 2. Inwentaryzacja serwerów 3. Inwentaryzacja urządzeń sieciowych 4. Inwentaryzacja systemów operacyjnych 5. Inwentaryzacja zainstalowanych aplikacji i pakietów 6. Inwentaryzacja dysków twardych 7. Inwentaryzacja plików 8. Inwentaryzacja drukarek 9. Inwentaryzacja wszystkich typów urządzeń również zasobów dodanych manualnie 10. Inwentaryzacja materiałów eksploatacyjnych (Magazyn IT) 11. Skaner środowisk wirtualnych (API) 12. Inwentaryzacja Hyper-V i VMWare 13. Inwentaryzacja i monitorowanie uprawnień do zasobów lokalnych oraz udostępnionych (ACL Manager) 14. Magazyn IT, prowadzenie ewidencji ilościowo-wartościowej 15. Baza CMDB |
| Monitorowanie IT | 1. Skaner sieci i mapy sieci (obsługa SNMP v1, v2c, v3) 2. Monitorowanie sieci 3. Monitorowanie usług sieciowych 4. Monitorowanie komputerów 5. Monitorowanie pracy pracowników 6. Monitorowanie uprawnień ACL 7. Monitorowanie odwiedzanych stron WWW 8. Monitorowanie urządzeń USB 9. Monitorowanie poczty Outlook 10. Monitorowanie sesji RDP 11. Monitorowanie uruchamianych procesów 12. Monitorowanie transferu sieciowego 13. Monitorowanie drukarek sieciowych 14. Monitorowanie drukowania 15. Monitorowanie wydajności 16. Monitorowanie usług 17. Monitorowanie dzienników zdarzeń 18. Monitorowanie sensorów 19. Monitorowanie serwisów WWW 20. Kreator raportów |
| Zarządzanie IT | 1. Zdalne zarządzanie komputerami (RDP, VNC, Intel vPro) 2. Zdalne zarządzanie zaporą (firewall) 3. Zdalny dostęp do edytora rejestrów/usług/procesów systemowych 4. Automatyzacja zadań administratora 5. Zarządzanie oprogramowaniem i licencjami 6. Deinstalacja oprogramowania / Automatyczna deinstalacja oprogramowania 7. Skaner maszyn wirtualnych 8. Komunikator 9. Powiadomienia administracyjne 10. Wbudowany harmonogram importu |

# Wdrożenie i konfiguracja elementów bezpieczeństwa

## Oprogramowanie do monitoringu zasobów IT

W ramach wdrożenia Zamawiający oczekuje:

1. Utworzenia maszyn wirtualnych do instalacji oprogramowania,
2. Instalacji i wstępnej konfiguracji oprogramowania,
3. Parametryzacji oprogramowania zgodnie z przygotowanym projektem, co najmniej w zakresie:
   1. Monitoring zasobów serwerowych (CPU, RAM, pamięć masowa),
   2. Monitoring dostępności wszystkich hostów,
   3. Monitoring dostępności usług WWW,
   4. Konfiguracja kokpitów,
   5. Konfiguracja powiadomień.
4. Przeprowadzenie testów systemu,
5. Przeprowadzanie szkoleń stanowiskowych dla administratora.

## System klasy SIEM

Wdrożenie oprogramowania SIEM zgodnie z założeniami projektowymi, co najmniej w zakresie:

1. Instalacja oprogramowania SIEM.
2. Integracja z systemem centralnego zarządzania tożsamością.
3. Integracja z oprogramowaniem do zarządzania incydentami.
4. Przygotowanie instrukcji instalacji agentów system SIEM oraz wsparcie przy instalacji pierwszego agenta dla każdego typu wspieranego systemu operacyjnego.
5. Przygotowanie obsługi do 5 niestandardowych źródeł logów (dekodery i reguły).
6. Określenie technik i taktyk ataku zgodnie z MITRE ATT&CK dla wszystkich niestandardowych reguł, które będą tego wymagały.
7. Określenie priorytetów alarmów w celu ograniczenia „szumu informacyjnego” i eskalacji istotnych alertów.
8. Konfiguracja mechanizmów agenta SIEM do czasowego blokowania źródłowych adresów IP wykonujących brute force.
9. Konfiguracja do 2 kokpitów.
10. Konfiguracja powiadomień mailowych.

## Platforma szkoleniowa

W ramach realizacji PZ Wykonawca jest zobowiązany do opracowania i wdrożenia w postaci kursu LMS materiałów szkoleniowych dla pracowników Zamawiającego. Zamawiający planuje wykorzystać system LMS do realizacji wstępnych oraz okresowych szkoleń dla swoich pracowników z tematyki cyberbezpieczeństwa. Zakres wdrożonego kursy musi być tożsamy z wymaganiami dotyczącymi szkoleń dla pracowników nie będących informatykami. Dodatkowo Wykonawca jest zobowiązany przygotować testy wiedzy oraz wdrożyć opcjonalny mechanizm testów w ramach LMS.

# Opracowanie SZBI oraz aktualizacja PBI dla Urzędy oraz 5 jednostek podległych

W ramach realizacji przedmiotu zamówienia Wykonawca musi opracować na podstawie danych od Zamawiającego następujące dokumenty będące podstawą SZBI:

1. Deklaracja najwyższego kierownictwa
2. Polityka Bezpieczeństwa Informacji
3. Procedura zarządzania ciągłością działania
4. Procedura zarządzania incydentami
5. Procedura bezpieczeństwa fizycznego
6. Procedura bezpieczeństwa teleinformatycznego
7. Procedura zarządzania uprawnieniami
8. Procedura zarządzania ryzykiem
9. Procedura realizacji działań naprawczych
10. Procedura klasyfikacji informacji
11. Procedura audytów wewnętrznych
12. Procedura bezpieczeństwa dostępu zdalnego

Dokumenty muszą być opracowane we współpracy z Zamawiającym, z uwzględnieniem otrzymanych od Zamawiającego wytycznych oraz wzorców, wytycznych audytu bezpieczeństwa i zostać zatwierdzone ostatecznie przez Zamawiającego.

Opracowana dokumentacja musi uwzględniać techniczne wytyczne, specyfikę wdrażanego sprzętu i oprogramowania oraz ewentualne ograniczenia. Zamawiający oczekuje otrzymania dokumentów, których stosowanie będzie możliwe wprost przy udziale wdrażanego w ramach PZ systemów.

Dokumentacja musi być przygotowana dla Urzędu Gminy oraz 5 jednostek podległych.