Zamówienie finansowane ze środków FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Poprawa bezpieczeństwa – obszar techniczny

Zadanie nr 1. Oprogramowanie do kopii zapasowych wraz ze wsparciem

- Możliwość backupu 30 komputerów, 3 serwerów, 2 hostów wirtualizacji edycja Professional
- Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich
- Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, 2025, Linux, BSD, Mac OS X, QNAP, Synology
- Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, 2025, Linux, BSD, Mac OS X, QNAP, Synology
- Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
- Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
- Automatyczny backup przy wyłączaniu komputera
- Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
- Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
- Backup baz danych i plików poczty w trybie online i offline
- Kopie rotacyjne (wersjonowanie)
- Zapis archiwów w otwartym formacie (ZIP 64-bit)
- Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
- Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
- Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
- Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
- Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
- Kompresja po stronie stacji roboczej
- Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
- Centralne sterowanie całym Systemem z jednego miejsca

- Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
- Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
- Wysyłanie Alertów administracyjnych na e-mail
- Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
- Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
- Automatyczna aktualizacja oprogramowania na komputerach zdalnych
- Interfejs, instrukcja i pomoc techniczna w języku polskim
- Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)
- Możliwość instalacji klienta przez GPO
- Współpraca z systemami Systemami Zarządzania Informacją i Zdarzeniami Bezpieczeństwa (SIEM - Security Information and Event Management)
- Możliwość zastosowania własnych certyfikatów SSL
- **Bezterminowa licencja - licencja nie może być ograniczona czasowo**
- Wsparcie techniczne obejmujące m.in. pełną **analizę problemu**, rozwiązywanie konkretnych problemów z konfiguracją programu lub systemu operacyjnego oraz przygotowanie i natychmiastowe udostępnienie poprawek do błędów krytycznych. Wsparcie w tym zakresie świadczone do 30 czerwca 2026 r., po tym okresie wsparcie świadczone w ramach licencji, obejmujące instalację, konfigurację oraz pomoc w rozwiązywaniu typowych problemów z obsługą programu. Pomoc świadczona jest w godzinach pracy telefonicznie i poprzez e-mail.

Zadanie nr 2. Systemem do zbierania i analizy logów

1. **Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:**
   1.1. System operacyjny powinien być na licencji Open Source.
   1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego fizyczny serwer z wirtualną maszyną będący na wyposażeniu Zamawiającego (do konfiguracji przez Dostawcę systemu).
   1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
   1.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć rozwiązanie sprzętowe o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.
   1.5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
   1.6. 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.

1.7. 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.

1.8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.

1.9. 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.

1.10. 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 (dashboardów).

2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:

2.1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego serwerze fizyczny z maszyną wirtualną.

2.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.

2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

- (1x) Urządzenie klasy UTM firmy Fortigate
- (6x) Przełączniki zarządzalne firmy Ubiquiti
- (2x) Serwery Windows
- (30x) stacji roboczych Windows 10 i 11
- (1x) Aplikację centralnego zarządzania ESET Endpoint Security
- (4x) Serwer wirtualizacji

2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.

2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.

2.8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
2.9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
2.10. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
2.11. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

3. Szkolenie w formie warsztatu:
3.1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zmawiającego warsztaty techniczne z zarządzenia i administracji wdrożonego systemu.
3.2. Zamawiający wymaga aby usługa została zrealizowana w terminie do 6 miesięcy od zamówienia usługi (nie później niż do 30 czerwca 2026 r.).
3.3. Zamawiający wymaga przeszkolenia w formie warsztatów jednego uczestnika.
3.4. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
3.5. Wymagana agenda warsztatów:
- Wstęp do zarządzania logami
- Wymagania oraz architektura wdrożonego rozwiązania
- Instalacja i konfiguracja ogólnych ustawień
- Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
- Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie
- Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych
- Konfiguracja alertów i powiadomień.
- Administracja i utrzymanie wdrożonego rozwiązania
- Case Study czyli praktyczne przykłady użycia

3.6. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
3.7. Zamawiający wymaga aby wykonawca pokrył koszty pełnego wyżywienia i zakwaterowania uczestnika w czasie warsztatów.
3.8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu.

4. Gwarancja i asysta techniczne:
4.1. Zamawiający wymaga aby Wykonawca w czasie 24 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
4.2. Zamawiający wymaga aby Wykonawca w okresie 24 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
4.3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.

4.4. Zamawiający akceptuje fakt, ze 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.

Zadanie nr 3. Serwer do systemu zbierania i analizy logów (1 sztuka)

Lp.	Parametry	Charakterystyka (wymagania minimalne)
3.1	**Obudowa**	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
3.2	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.3	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
3.4	**Procesor**	Zainstalowane dwa procesory 8-rdzeniowe, min. 2.8 GHz (Turbo Speed min. 3.6 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 30700 w teście Average CPU Mark dostępnym na stronie dla konfiguracji dwu procesorowej https://www.cpubenchmark.net/
3.5	**RAM**	32GB DDR4 RDIMM 3200MT/s, w modułach 16GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
3.6	**Funkcjonalność pamięci RAM**	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
3.7	**Gniazda PCI**	- minimum dwa sloty PCIe x16 generacji 4
3.8	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.
3.9	**Dyski twarde**	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 4 dyski HDD SAS o pojemności min. 600GB, 12Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. 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 wnęk na dyski twarde

3.10	**Kontroler RAID**	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
3.11	**System operacyjny/System wirtualizacji**	Windows Server 2025 w wersji STD. Na serwerze wykonawca zainstaluje dwa środowiska wirtualne: Linux i Windows Server 2025 STD
3.12	**Wbudowane porty**	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
3.13	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
3.14	**Wentylatory**	Redundantne
3.15	**Zasilacze**	Redundantne, Hot-Plug maksymalnie 700W.
3.16	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
3.17	**Diagnostyka**	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
3.18	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

		• szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
3.19	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019.
3.20	**Warunki gwarancji**	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga, aby, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostał u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz

		pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
3.21	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Zadanie nr 4. Usługa konfiguracja UTM (aktualnie posiadanego tj. Fortigate)

- aktualizacja oprogramowania do najnowszej stabilnej wersji
- przegląd konfiguracji i optymalizacja ustawień
- konfiguracja interfejsów sieciowych
- konfiguracja serwera dhcp
- konfiguracja serwera dns
- ustawienia uprawnień administracyjnych
- tworzenie profili zarządzania
- tworzenie kont użytkowników zarządzających
- konfiguracja usługi FortiGuard
- rejestracja licencji, konfiguracja mechanizmów fortiguard
- konfiguracja routingu statycznego
- opcja* konfiguracja 2 niezależnych łącz oraz możliwości redundancji / balansowania
- konfiguracja polityk bezpieczeństwa
- konfiguracja obiektów
- konfiguracja przekierowania portów
- konfiguracja profili AV
- konfiguracja profili web filter
- konfiguracja profili application control
- konfiguracja profili intrusion protection
- konfiguracja profili data leak prevention
- konfiguracja i podłączenie do forticloud
- konfiguracja wykrywania urządzeń oraz grupowanie list dostępu
- konfiguracja polityk bezpieczeństwa w oparciu o adresy
- konfiguracja polityk bezpieczeństwa w oparciu o użytkowników
- konfiguracja polityk bezpieczeństwa w oparciu o urządzenia
- instalacja i konfiguracja oprogramowania forticlient
- konfiguracja połączeń VPN IPsec

- konfiguracja połączeń SSL.VPN
- opcja* konfiguracja połączeń VPN Ipsec między urządzeniami
- konfiguracja skanowania podatności
- wsparcie w obsłudze i konfiguracji do 30 czerwca 2026 r.