Szczegółowy opis przedmiotu zamówienia

Spis treści

Zadanie 1 Zakup i konfiguracja FortiAnalyzera

Wymagania Ogólne

Zamawiający wymaga dostarczenia dla Urzędu Miasta i Gminy Mirsk FortiAnalyzera wraz ze wsparciem oraz konfiguracją wirtualnego rozwiązania do centralnego zbierania i analizy logów z urządzeń sieciowych i zabezpieczających, wraz z licencją umożliwiającą przetwarzanie dodatkowych 5 GB logów dziennie oraz wsparciem technicznym klasy premium od dnia podpisania umowy do 31.05.2026r.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.x,6.x,7.0.x,8.0.x; Microsoft Hyper-V wersje: 2016, 2019, 2022 i 2025; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).Interfejsy, Dysk:

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

Podstawowe funkcje:

- Centralne gromadzenie, agregacja i analiza logów z urządzeń zabezpieczających i sieciowych.
- Zaawansowane funkcje korelacji zdarzeń, wykrywania zagrożeń i generowania raportów bezpieczeństwa.
- Obsługa środowisk wirtualnych z możliwością wdrożenia jako maszyna wirtualna.
- Dostęp do interfejsu webowego do zarządzania, konfiguracji i monitoringu.
- Zapewnienie zgodności z obowiązującymi regulacjami dotyczącymi przechowywania i analizy logów.
- System musi być w stanie umożliwiać skalowanie i przyjmować minimum 5 GB logów na dzień.
- Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie:

- Podgląd logowanych zdarzeń w czasie rzeczywistym.
- Możliwość przeglądania logów historycznych z funkcją filtrowania.
- System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
  a. Listę najczęściej wykrywanych ataków.
  b. Listę najbardziej aktywnych użytkowników.
  c. Listę najczęściej wykorzystywanych aplikacji.
  d. Listę najczęściej odwiedzanych stron www.
  e. Listę krajów , do których nawiązywane są połączenia.
  f. Listę najczęściej wykorzystywanych polityk Firewall.
  g. Informacje o realizowanych połączeniach IPSec.
- Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
- Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
- System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

W zakresie raportowania system musi zapewniać:

- Generowanie raportów co najmniej w formatach: PDF, CSV.
- Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
- Funkcję definiowania własnych raportów.

- Możliwość spolszczenia raportów.
- Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

W zakresie korelacji zdarzeń system musi zapewniać:

Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

- Malware.
- Aplikacje sieciowe.
- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

- System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

- System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

- Wsparcie: System musi być objęty serwisem producenta przez okres od dnia podpisania umowy do 31.05.2026r. upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

- Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
- Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Zadanie 2 Zakup oraz instalacja aplikacji do backupu i odzyskiwania danych

Zadanie 2.1 Dostawa oraz wdrożenie oprogramowanie do kompleksowej ochrony danych w środowiskach wirtualnych, fizycznych i chmurowych wraz z rocznym wsparciem technicznym

Przedmiot zamówienia:

Dostawa licencji wieczystej dla Urzędu Miasta i Gminy Mirsk na oprogramowanie wraz z wdrożeniem do kompleksowej ochrony danych w środowiskach wirtualnych, fizycznych i chmurowych – pakiet 10 instancji, wersja zaawansowana, wraz ze wsparciem technicznym od dnia podpisania umowy do dnia 31.05.2026r.

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa licencji wieczystej na pakiet 10 instancji oprogramowania do tworzenia kopii zapasowych, odzyskiwania danych oraz zaawansowanego monitorowania i analizy środowiska backupowego, przeznaczonego do ochrony danych w środowiskach wirtualnych, fizycznych oraz chmurowych.

Licencja powinna obejmować pełen zestaw funkcji umożliwiających:

- Tworzenie i zarządzanie kopiami zapasowymi maszyn wirtualnych działających na platformach VMware vSphere, Microsoft Hyper-V, Nutanix AHV oraz innych popularnych hypervisorach.
- Backup serwerów fizycznych z systemami Windows i Linux oraz stacji roboczych.
- Backup danych przechowywanych w środowiskach chmurowych, takich jak AWS, Microsoft Azure, Google Cloud i IBM Cloud.
- Ochronę danych aplikacji i baz danych (np. Microsoft SQL, Oracle, SAP HANA, PostgreSQL, MySQL, IBM Db2, MongoDB).
- Backup i przywracanie danych z urządzeń NAS oraz zasobów nieustrukturyzowanych (np. plików i folderów).
- Licencja w wersji zaawansowanej powinna zawierać dodatkowo:
- Zaawansowane narzędzia do monitorowania, raportowania oraz analizy środowiska backupowego, umożliwiające proaktywne wykrywanie i rozwiązywanie problemów zanim wpłyną one na ciągłość działania systemów.
- Możliwość generowania rozbudowanych raportów, alertów oraz wizualizacji trendów dotyczących wydajności, wykorzystania zasobów i stanu środowiska ochrony danych.
- Automatyzację i optymalizację procesów backupu, w tym zarządzanie kopiami zapasowymi w środowiskach hybrydowych (lokalnych i chmurowych).
- Integrację z narzędziami do monitoringu i zarządzania infrastrukturą IT, umożliwiającą centralne zarządzanie i analizę danych backupowych.
- Obsługę zaawansowanych scenariuszy ochrony danych, w tym replikacji, backupu ciągłego oraz elastycznego zarządzania pojemnością licencji.

- Licencja wieczysta na pakiet 10 instancji, umożliwiająca ochronę dowolnych obciążeń (maszyn wirtualnych, serwerów fizycznych, stacji roboczych, aplikacji, zasobów chmurowych).
- Licencja powinna być zgodna z modelem uniwersalnym, umożliwiającym przenoszenie licencji między różnymi typami obciążeń.

Zadanie 2.2 Dostawa oraz wdrożenie oprogramowanie do kompleksowej ochrony danych w środowiskach wirtualnych, fizycznych i chmurowych wraz z rocznym wsparciem technicznym

Przedmiot zamówienia:

Dostawa licencji wieczystej dla Zakładu Gospodarki Komunalnej i Mieszkaniowej w Mirsku na oprogramowanie wraz z wdrożeniem do ochrony danych – pakiet 10 instancji, wersja podstawowa, wraz ze wsparciem technicznym od dnia podpisania umowy do dnia 31.05.2026r.

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest licencja wieczysta na pakiet 10 instancji oprogramowania do tworzenia kopii zapasowych i odzyskiwania danych, przeznaczonego do podstawowej ochrony środowisk IT obejmujących systemy wirtualne, fizyczne oraz chmurowe.
Licencja ta umożliwia:

- Tworzenie kopii zapasowych i odzyskiwanie danych maszyn wirtualnych działających na platformach VMware vSphere, Microsoft Hyper-V oraz Nutanix AHV.
- Backup serwerów fizycznych z systemami operacyjnymi Windows i Linux oraz stacji roboczych.
- Ochronę danych w środowiskach chmurowych, takich jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud oraz IBM Cloud.
- Backup i odzyskiwanie danych aplikacji i baz danych, w tym Microsoft SQL Server, Oracle, SAP HANA, PostgreSQL, MySQL, IBM Db2 oraz MongoDB.
- Backup i przywracanie danych z urządzeń NAS oraz zasobów plikowych i folderów.

Wersja podstawowa zapewnia stabilne i niezawodne podstawowe funkcje backupu i odzyskiwania danych, bez wbudowanych zaawansowanych narzędzi do monitorowania

i analizy środowiska backupowego. Oferuje podstawowe raportowanie i zarządzanie kopiami zapasowymi, umożliwiając skuteczne zabezpieczenie danych, ale nie zawiera rozbudowanych mechanizmów proaktywnego wykrywania problemów, zaawansowanych alertów ani wizualizacji trendów.

Licencja jest wieczysta, co oznacza jednorazowy zakup z prawem do nieograniczonego użytkowania oprogramowania.

Licencja jest uniwersalna, co pozwala na przenoszenie uprawnień pomiędzy różnymi typami obciążeń, takimi jak maszyny wirtualne, serwery fizyczne, aplikacje czy zasoby chmurowe.

Zadanie 3 Zakup licencji aplikacji w zakresie bezpieczeństwa ochrony danych i monitorowania oraz jej instalację

Przedmiotem zamówienia jest dostawa dla Urzędu Miasta i Gminy Mirsk oraz instalacja oprogramowania do automatycznego zarządzania i koordynacji procesów odzyskiwania danych w środowiskach wirtualnych i chmurowych, wraz z licencją użytkowania od dnia podpisania umowy do dnia 31.05.2026r.

Wymagania funkcjonalne oprogramowania:

- Musi tworzyć jednolitą platformę funkcjonalną z oprogramowaniem z części 2.1.
- Automatyczne testowanie i weryfikacja planów odzyskiwania danych bez wpływu na środowisko produkcyjne.
- Możliwość zarządzania procesami odzyskiwania dla maszyn wirtualnych działających na platformach wirtualizacyjnych typu VMware vSphere, Microsoft Hyper-V oraz środowisk chmurowych (np. Microsoft Azure).
- Automatyczne generowanie i aktualizacja dokumentacji planów odzyskiwania w celu zapewnienia zgodności z wymogami audytowymi i biznesowymi.
- Obsługa planowania i wykonywania testów odzyskiwania w izolowanych środowiskach testowych.
- Raportowanie zgodności z określonymi wskaźnikami RTO (Recovery Time Objective) i RPO (Recovery Point Objective).
- Integracja z systemami do backupu i monitoringu środowiska IT.

Uzasadnienie wykorzystania znaków towarowych i nazw własnych

Zamawiający w przedmiocie zamówienia wskazuje znaki towarowe, patenty, pochodzenie i nazwy własne charakteryzujące produkty w celu wystarczająco precyzyjnego wskazania przedmiotu zamówienia jednakże dopuszcza rozwiązania „równoważne". Zamawiający wskazał we wniosku o dofinansowanie konkretne potrzeby dla poszczególnych jednostek. Wskazanie znaków towarowych i nazw własnych w zamówieniu jest uzasadnione koniecznością zapewnienia kompatybilności, efektywności operacyjnej oraz zgodności technicznej z posiadanym sprzętem i oprogramowaniem. Sprzęt oraz oprogramowanie od uznanych producentów zapewnią odpowiedni poziom zabezpieczeń i stabilności systemów. Wybór konkretnych rozwiązań, poprzez użycie ich nazw, gwarantuje nieprzerwaną i bezpieczną pracę.