Wymagania minimalne dla zadania:

Wdrożenie systemu zapobiegającego wyciekowi danych klasy DLP wraz ze szkoleniem.

Cel Zamówienia:

Wdrożenie systemu zapobiegającego wyciekowi danych klasy DLP wraz ze szkoleniem.

Licencja na:

- 120 stanowisk
- 24 miesiące od dnia dostawy przez wykonawcę.

Wykonawca zobowiązuję się do wdrożenia zakupionego systemu – minimum 2 godziny, zdalnie.

Wykonawca zobowiązany jest do przeszkolenia dwóch osób z obsługi systemu DLP zgodnie z poniższą specyfikacją.

Specyfikacja systemu klasy DLP

	Wymagania minimalne
Ochrona przed wyciekiem danych	1. Pełne wsparcie dla stacji roboczych z systemami Windows 10/11. 2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych. 3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim. 4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim. 5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL oraz AzureSQL. 6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta. 7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych. 9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym. 10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu

	ponownego połączenia z serwerem administracyjnym. 11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol. 12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące. 13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy. 14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania oraz edycji wyżej wymienionych kategorii. 15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania. 16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na: • Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module, • Logi, które określają możliwość wyświetlenia logów poszczególnego modułu. 17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory. 18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej: • logowanie oraz wylogowanie użytkownika, • włączenie oraz wyłączenie stacji roboczej, • blokada oraz odblokowanie stacji roboczej, • przejście w stan bezczynności stacji roboczej. 19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym. 20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji. 21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje,

	podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach. 22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików. 23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF oraz XLS. 24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu. 25. Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email. 26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach. 27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu. 28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail. 29. Serwer administracyjny musi posiadać domyślnie skonfigurowany serwer SMTP udostępniony przez producenta oprogramowania. 30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku. 31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików. 32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o: • aplikacje, z której zostały utworzone, • lokalizację, • adres URL, • format pliku, • zawartość pliku. 33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych. 34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł: • blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych

	dyskach lokalnych,
	• blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
	• blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
	• blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
	• blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
	• blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
	• blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
	  • Dropbox,
	  • Google Drive,
	  • SharePoint
	  • OneDrive Business,
	  • OneDrive Personal.
	• blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
	• blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
	• blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
	• uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
	35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
	36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
	37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
	38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
	39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
	40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o

	określonych literach oraz folderów synchronizacji z usługami chmury. 41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT. 42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM. 43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika. 44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych. 45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o: • numery kart kredytowych, • numer PESEL, • numer polskiego dowodu osobistego, • polski numer paszportu, • wyrażenia regularne, • określone ciągi znaków, • numer IBAN. 46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition) ze wsparciem języka polskiego. 48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych. 49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e- mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”). 50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania). 51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate. 52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM. 53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików. 54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:

	• audyt i logowanie wiadomości e-mail, • audyt operacji na plikach Sharepoint Online. 55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau). 56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi. 57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na: • Bezpieczeństwo danych: • Przegląd informacji o incydentach bezpieczeństwa. • Przegląd danych przychodzących. • Przegląd danych wychodzących. • Podłączane/odłączane urządzenia przenośne. • Produktywność: • Przegląd informacji na temat produktywności użytkowników. • Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. • Trendy. • Eksploatacja sprzętu: • Przegląd informacji na temat eksploatacji sprzętu komputerowego. • Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. • Eksploatacja drukarek. • Eksploatacji sieci. 58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP. 59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania. 60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt: • plików przenoszonych na nośniki USB i inne urządzenia przenośne, • plików przesłanych za pomocą wiadomości e-mail, • plików przesłanych za pomocą poczty webowej, • plików przesłanych do Internetu, • plików wysłanych za pomocą komunikatorów, • plików przesłanych na dyski chmurowe, • analiza sposobu korzystania z aplikacji, • analiza korzystania z Internetu, • analiza wykorzystania portali do poszukiwania pracy. 61. Konsola aplikacyjna musi umożliwiać możliwość konfiguracji podwójnej autoryzacji

	62. Konsola aplikacyjna musi umożliwiać konfigurację dwóch języków dla mechanizmu OCR

Szkolenie dla administratorów systemu klasy DLP

Wymagania minimalne	
Informacje ogólne	• Szkolenie dla dwóch osób • Szkolenie w trybie stacjonarnym, • Czas trwania szkolenia: minimum 2 dni (14 godzin) • Szkolenie musi przeprowadzone przez autoryzowane centrum szkoleniowe producenta zakupionego systemu DLP • Prowadzący szkolnie muszą posiadać certyfikaty do przeprowadzania autoryzowanych szkoleń wystawione przez producenta zakupionego systemu DLP. • Oferta powinna zawierać wspomniane certyfikaty, jak również szczegółowy program szkolenia.
Program szkolenia powinien zawierać minimum takie zagadnienia	Podstawowe informacje o systemie DLP: • Licencjonowanie • Wspierane systemy operacyjne Wdrożenie rozwiązania systemu DLP: • Omówienie instalatora systemu DLP • Wdrożenie modułu zarządzania • Wdrożenie agentów na stacjach roboczych Omówienie modułów systemu DLP zawierających takie zagadnienia: • Analiza wycieków danych • Filtrowanie i raporty • Szyfrowanie BitLockerem, ochrona dysków • Konfiguracja dostępu do urządzeń i portów Omówienie modułu webowego systemu DLP: • Minimalne wymagania systemowe • Instalacja oraz konfiguracja modułu webowego • Analiza zachowań • Zarządzenie kategoriami produktywności • Kontrola WWW i aplikacji • Alerty, raporty i konserwacja Zaawansowane funkcje systemu DLP: • Reguły DLP • Reguły ogólne

	• Reguły aplikacji • Inteligentne wyszukiwanie danych osobowych • Czym są tagi i do czego służą • Reguły tagowania dla aplikacji, stron oraz lokalizacji • Dzienniki systemu DLP