

OPIS PRZEDMIOTU ZAMÓWIENIA

„DOSTAWA I WDROŻENIE OPROGRAMOWANIA DLP (DLP – DATA LEAK PREVENTION)
DLA WOJEWÓDZKIEGO INSPEKTORATU TRANSPORTU DROGOWEGO W OPOLU”

1. Dostawa i wdrożenie oprogramowania **DLP (Data Leak Prevention)** spełniającego niżej wymienione minimalne parametry:

LP.	PARAMETR	WYMAGANIA TECHNICZNE
1	PARAMETRY MINIMALNE	<p>System DLP na 70 urządzeń z wieczystą licencją i wsparciem na 12 miesięcy:</p> <ol style="list-style-type: none"> System operacyjny: <ol style="list-style-type: none"> Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi MacOS 12 lub nowszy. Serwer administracyjny musi obsługiwać instalację na systemach: <ol style="list-style-type: none"> Windows Server 2016(64-bit) i nowszych. Serwer administracyjny musi obsługiwać bazy danych: <ol style="list-style-type: none"> MS SQL Server 2016 lub nowsze, MS SQL Express, c. AzureSQL S3 lub nowsze. Pomoc i dokumentacja programu dostępne w języku angielskim. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta nastacjach roboczych. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategorizowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.
33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.

		<p>34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.</p> <p>35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)</p> <p>36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.</p>
	OPIS WDROŻENIA I SZKOLENIA DLP	<p>1. Zainstalowanie serwera oraz agentów i klientów na końcówkach, celem zbierania informacji oraz omówienie konsoli oprogramowania.</p> <p>2. Przeanalizowanie potencjalnych miejsc wycieków danych oraz wygenerowanie przykładowego audytu, stworzenie klasyfikacji danych (maksymalnie trzech).</p> <p>3. Utworzenie polityki egzekwowanych na stacjach końcowych (maksymalnie 3) na podstawie klasyfikacji z poprzedniego modułu, dodatkowo optymalizując działanie systemu.</p>
2	PLAN WDROŻENIA	<p>1. Instalacja i konfiguracja serwera DLP– oprogramowania zarządzającego.</p> <p>2. Omówienie procedury instalacyjnej klientów oraz ustawienie zadania wdrożenia na innych komputerach.</p> <p>3. Integracja z Active Directory.</p> <p>4. Omówienie funkcji konsoli zarządzającej.</p> <p>5. Analiza środowiska i włączenie funkcji audytowania.</p> <p>6. Podstawowa analiza wycieków danych z maksymalnie jednej przykładowej stacji roboczej.</p> <p>7. Wygenerowanie przykładowego raportu audytu.</p> <p>8. Ustawienie klasyfikacji danych (maksymalnie trzech) w oparciu o wskazane przez klienta dane wrażliwe.</p> <p>9. Wdrożenie maksymalnie trzech polityk DLP (np. pochodzenia pliku, zawartości pliku, właściwości pliku).</p> <p>10. Wdrożenie kontroli dostępu do stron WWW i urządzeń przenośnych.</p> <p>11. Końcowe testy i optymalizacja ustawień.</p>
3	ZAKRES SZKOLENIA	<p>Szkolenie z obsługi i konfiguracji oprogramowania DLP dla jednego administratora:</p> <p>Moduł 1. Podstawowe informacje:</p> <p>1. Licencjonowanie;</p> <p>2. Wspierane systemy operacyjne.</p> <p>Moduł 2. Wdrożenie rozwiązania:</p> <p>1. Omówienie instalatora;</p> <p>2. Wdrożenie serwera;</p> <p>3. Wdrożenie klienta.</p> <p>Moduł 3. Konsola:</p> <p>1. Kategoryzacja aplikacji oraz stron internetowych;</p> <p>2. Zarządzanie bazą danych;</p> <p>3. Ustawienia klienta;</p> <p>4. Dezaktywacja modułów klienta;</p> <p>5. Ustawienia integracji.</p>

		<p>Moduł 4. Moduł Discovery:</p> <ol style="list-style-type: none">1. Uruchomienie modułu Discovery;2. Analiza potencjalnych wycieków danych;3. Dostosowanie konsoli do własnych potrzeb, filtrowanie danych. <p>Moduł 5. Podstawowe dla DLP:</p> <ol style="list-style-type: none">1. Szyfrowanie dysków BITLOCKEREM;2. Strefy - konfiguracja dostępów dla urządzeń i portów. <p>Moduł 6. Zaawansowane dla DLP:</p> <ol style="list-style-type: none">1. Reguły DLP – tryby polityk;2. Reguły ogólne;3. Reguły aplikacji;4. Kategorie danych;5. Inteligentne wykrywanie danych osobowych.
--	--	--