**Załącznik nr 1a**

**Opis przedmiotu zamówienia**

pn. Zakup systemu do ochrony przed wyciekami informacji wraz z wdrożeniem

1. **Funkcjonalności obligatoryjne**

|  |  |
| --- | --- |
| **Specyfikacja systemu ochrony przed wyciekiem informacji (DLP)** | **Spełnia: Tak/Nie** |
| 1. System musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
 |  |
| 1. System musi realizować swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer czy laptop (Endpoint DLP).
 |  |
| 1. Zarządzanie, konfiguracja polityk, obsługa incydentów oraz raportowanie muszą być spójne dla ochrony na poziomie sieci i stacji końcowych.
 |  |
| 1. Ochrona dla danych na poziomie sieci i stacji roboczych musi być realizowana z poziomu jednego zestawu polityk i reguł. Niedopuszczalne jest rozwiązanie, w którym polityki dla ochrony na poziomie sieci i stacji roboczych są osobnymi zestawami polityk.
 |  |
| 1. System musi umożliwiać monitorowanie i ochronę danych przesyłanych w kanałach komunikacyjnych, w szczególności:
	1. ruch webowy z wykorzystaniem protokołów HTTP oraz HTTPS,
	2. poczta elektroniczna – protokół SMTP.
 |  |
| 1. System musi mieć możliwość dodania predefiniowanych reguły ochrony oraz mechanizmy identyfikacji danych takich jak numery kart kredytowych, IBAN, oraz identyfikatorów jak PESEL, REGON, NIP, oraz numer dowodu osobistego.
 |  |
| 1. System musi umożliwiać:
	1. tworzenie własnych mechanizmów identyfikacji danych opartych o własne wzorce
	2. konfigurowalne mechanizmy walidacji.
 |  |
| 1. Ochrona informacji musi odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
 |  |
| 1. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
	1. Kto wysyła informacje,
	2. Dokąd informacje są wysyłane,
 |  |
| 1. System musi umożliwiać następujące reakcje na działania użytkownika naruszające polityki ochrony danych:
	1. zezwolenie działania,
	2. blokowanie działania,
	3. wysłanie zgodnych z przygotowanymi szablonami powiadomień, przy czym musi być możliwość selektywnego wysyłania powiadomień do:
		1. nadawcy, czyli osoby, która naruszyła politykę ochrony danych,
		2. administratora systemu DLP,
		3. dowolnego zdefiniowanego adresata.
 |  |
| 1. System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
	1. słowa kluczowe, frazy, słowniki,
	2. wyrażenia regularne,
	3. właściwości pliku takie jak nazwa, typ,
 |  |
| 1. Dodatkowo, w przypadku, gdy System działa w integracji z wspieranymi systemami klasyfikacji informacji, musi rozpoznawać etykiety klasyfikacji nadane plikom oraz wiadomościom e-mail i na tej podstawie egzekwować zdefiniowane polityki ochrony danych.
 |  |
| 1. Rozpoznawanie danych w plikach graficznych musi być również możliwe dla procesu przeszukiwania repozytoriów sieciowych takich jak serwery plików.
 |  |
| 1. System w zakresie ochrony danych na stacji końcowej musi umożliwiać monitorowanie takich czynności jak:
	1. kopiowanie informacji na zewnętrzne nośniki danych, np. pendrive,
	2. drukowanie zarówno na drukarki lokalne jak i sieciowe,
	3. kontrola aplikacji w zakresie operacji kopiuj/wytnij, wklej oraz dostęp aplikacji do pliku,
	4. kontrola treści przesyłanych za pomocą przeglądarki internetowej oraz klienta poczty,
	5. lokalne wykrywanie chronionych informacji w plikach na dysku stacji końcowej.
 |  |
| 1. System musi umożliwiać instalację agenta na komputerach z następującymi systemami operacyjnymi:
	1. Windows 7, 8, 8.1, 10, 11
	2. Windows Server 2012 R2, 2016, 2019
 |  |
| 1. Analiza danych przeprowadzana przez agenta systemu DLP na komputerze użytkownika musi być pełna i nie może wymagać przesyłania danych do bardziej szczegółowej analizy na serwerze systemu DLP. Agent systemu DLP musi zapewniać tak samo dobrą ochronę danych niezależnie od tego czy ma komunikację z serwerem systemu DLP czy nie.
 |  |
| 1. Maksymalny czas agregacji informacji o odnotowanych transmisjach chronionych treści nie może być krótszy niż 7 dni.
 |  |
| 1. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego.
 |  |
| 1. System musi umożliwiać wykrywanie danych na serwerach plików
 |  |
| 1. Dostęp do konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https.
 |  |
| 1. Dostęp do konsoli zarządzającej musi wymagać uwierzytelnienia. Oprócz hasła systemu DLP oraz hasła użytkownika z usługi katalogowej system DLP musi wspierać silne uwierzytelnianie cyfrowym certyfikatem użytkownika
 |  |
| 1. System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o role własne oraz wbudowane, takie jak administrator, audytor, manager incydentów.
 |  |
| 1. Konsola zarządzająca musi zawierać ekran przedstawiający podstawowe statystyki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.
 |  |
| 1. System DLP musi umożliwiać komunikację z użytkownikami końcowymi przynajmniej w języku polskim i angielskim. Wszystkie moduły programu muszą być dostępne przynajmniej w języku angielskim i/lub polskim.
 |  |
| 1. Dostarczona w ramach postępowania licencja musi umożliwiać użytkowanie wszystkich opisanych funkcjonalności przez okres co najmniej 1 roku od daty podpisania protokołu odbioru z możliwością późniejszego odnowienia.
 |  |
| 1. Przechowywanie logów Systemu DLP na serwerze przez okres co najmniej 90 dni. Możliwość przesyłania informacji o incydentach i zdarzeń systemowych do zewnętrznego serwera Syslog.
 |  |
| 1. System DLP należy dostarczyć i wdrożyć wraz całym wymaganym oprogramowaniem (bazy danych, systemy operacyjne itp.)
 |  |
| 1. Wykaz elementów podlegających ochronie przed wyciekiem danych:
	1. Ruch wychodzący na zewnątrz (**punkt 5**)
	2. Stacje robocze użytkowników w ilości ok. 200 szt.
	3. Serwer plików (Windows Server 2012 R2) 1 szt.
 |  |
| 1. Zakres wdrożenia:
	1. uruchomienie serwera i konsoli zarządzającej
	2. określenie odpowiedniej klasyfikacji elektronicznej wersji plików i dokumentów przetwarzanych przez Zamawiającego
	3. instalacja agenta na urządzeniach końcowych użytkownika na co najmniej 20 urządzeniach końcowych i 1 serwerze, przekazanie Zamawiającemu plików instalacyjnych, parametrów instalacji i instrukcji w celu samodzielnej instalacji na pozostałych urządzeniach
	4. Po wstępnej fazie pracy w trybie audytowania, podczas której wdrażana jest sieciowa kontrola DLP, należy przeprowadzić analizę pozyskanych danych. Powinno to obejmować zalecenia dotyczące działań ograniczających ryzyko, które mogą zmniejszyć częstość występowania danych na nie narażonych. Na tej podstawie należy dostosować początkowe polityki systemu DLP.
	5. instruktaż dla maksymalnie 4 osób wskazanych przez Zamawiającego w zakresie zarządzania, polityk, obsługi fingerprint-ów itp.
 |  |
| 1. Dokumentacja powykonawcza musi zawierać następujące elementy:
	1. **ogólny opis Systemu DLP.**
	2. **wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego Systemu DLP (w tym systemy operacyjne, bazy danych, serwery aplikacyjne, itp.)**
	3. **specyfikację techniczną, dostęp do dokumentacji technicznej www producenta**
	4. **instrukcje instalacyjne i instrukcje obsługi dla administratora systemu do ochrony przed wyciekiem danych,**
	5. **instrukcje obsługi dla użytkownika (operatora konsoli do obsługi incydentów),**
	6. **opis procedur archiwizacji i procedurę odtwarzania systemu jak i bazy zdarzeń/incydentów.**
 |  |

1. **Funkcjonalności punktowane**

|  |  |  |
| --- | --- | --- |
| **Specyfikacja systemu ochrony przed wyciekiem informacji (DLP)** | **Pkt** | **Spełnia: Tak/Nie** |
| 1. System musi umożliwiać definiowanie dodatkowych własnych kanałów transmisji, które mają być monitorowane np. protokół FTP, protokoły druku sieciowego LPD,LPR itp.
 | 5 pkt |  |
| 1. Architektura systemu DLP musi być modularna i umożliwiać wdrażanie kolejnych instancji jego modułów, w szczególności kolejnych serwerów systemu DLP, z możliwością delegowania ich do poszczególnych zadań zdefiniowanych w systemie DLP, w szczególności zadań tworzenia cyfrowych odcisków palców (ang. fingerprint) dla chronionych danych oraz wyszukiwania określonych danych na zasobach w sieci.
 | 2 pkt |  |
| 1. System musi zawierać wbudowane zestawy reguł i polityk oraz kreator ułatwiający ich wybór, które przyspieszają proces wdrożenia rozwiązania dostarczając ochrony dla popularnych typów danych, np. w celu uzyskania zgodności z różnymi regulacjami.
 | 2 pkt |  |
| 1. Dla wyżej wymienionych identyfikatorów System oprócz sprawdzenia ich zgodności z wzorcem musi walidować ich poprawność przez weryfikację zawartej w nich sumy kontrolnej.
 | 2 pkt |  |
| 1. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
 |
| * 1. W jaki sposób informacje są wysyłane (co najmniej w zakresie opisanym w **punkcie 5. a,b oraz 31. a**),
 | 3 pkt |  |
| * 1. Co jest wysyłane, czyli właściwa identyfikacja treści (co najmniej w zakresie opisanym w **punktach 11.a-c oraz 37.a-c**).
 | 3 pkt |  |
| 1. System musi umożliwiać następujące reakcje na działania użytkownika naruszające polityki ochrony danych:
 |
| * 1. kwarantannę wiadomości e-mail,
 | 1 pkt |  |
| * 1. szyfrowanie wiadomości e-mail oraz plików kopiowanych na zewnętrzne nośniki danych,
 | 1 pkt |  |
| * 1. umożliwienie użytkownikowi kontynuowania operacji po podaniu uzasadnienia i zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na komputerze użytkownika,
 | 1 pkt |  |
| * 1. wysłanie zgodnych z przygotowanymi szablonami powiadomień, przy czym musi być możliwość selektywnego wysyłania powiadomień do:
 |
| * + 1. przełożonego (menadżera, kierownika) nadawcy,
 | 1 pkt |  |
| * + 1. właściciela danych zdefiniowanego w polityce chroniącej określone dane, np. Dział Kadr w przypadku danych osobowych pracowników,
 | 1 pkt |  |
| 1. System musi umożliwiać łączenie polityk w grupy.
 | 1 pkt |  |
| 1. System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
 |
| * 1. tworzenie odcisku palca – fingerprint, polegającej na tworzeniu cyfrowej reprezentacji danych zawartych w dokumencie lub w bazie danych z wykorzystaniem jednokierunkowej funkcji skrótu – hash,
 | 1 pkt |  |
| * 1. skrypty umożliwiające rozpoznanie identyfikatorów takich jak PESEL, REGON, NIP, czy numer karty kredytowej wraz z zweryfikowaniem poprawności tego identyfikatora poprzez np. sprawdzenie zaszytej w nim sumy kontrolnej,
 | 1 pkt |  |
| * 1. możliwość wytrenowania systemu DLP tak, aby odróżniał dokumenty określonego rodzaju tworzone w ramach organizacji od innych dokumentów tego samego typu poprzez zaprezentowanie odpowiednich zestawów dokumentów treningowych.
 | 2 pkt |  |
| 1. System musi umożliwiać łączenie w politykach wielu mechanizmów identyfikacji danych wyrażeniami logicznymi pozwalając na reagowanie w przypadku wystąpienia określonej kombinacji chronionych danych.
 | 1 pkt |  |
| 1. System musi umożliwiać tworzenie fingerprint zarówno dla danych ustrukturyzowanych takich jak bazy danych oraz pliki csv jak i dla danych nieustrukturyzowanych takich jak pliki.
 | 1 pkt |  |
| 1. Tworzenie fingerprint-ów dla danych ustrukturyzowanych musi być możliwe w odniesieniu do:
 |
| * 1. Baz danych
 | 1 pkt |  |
| * 1. Plików CSV
 | 1 pkt |  |
| 1. Tworzenie fingerprint-ów dla danych nieustrukturyzowanych musi być możliwie dla serwerów plików.
 | 2 pkt |  |
| 1. Algorytm tworzenia fingerprint dla pliku musi tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości.
 | 1 pkt |  |
| 1. Dla plików niezawierających tekstu np. binarnych lub graficznych musi być możliwe tworzenie odcisku palca dla całego dokumentu, aby możliwe było wykrycie jego transmisji lub użycia w całości.
 | 1 pkt |  |
| 1. System musi umożliwiać wykrywanie chronionych treści w przesyłanych plikach graficznych wykorzystując technologię OCR (ang. optical character recognition). Wspomniana analiza musi odbywać się na dedykowanym serwerze, aby nie obciążać agenta na stacji roboczej.
 | 1 pkt |  |
| 1. System w zakresie ochrony danych na stacji końcowej musi umożliwiać monitorowanie nagrywania płyt CD/DVD
 | 1 pkt |  |
| 1. W zakresie wysyłania danych przez przeglądarkę internetową agent systemu DLP na komputerze użytkownika musi umożliwiać analizę i wykrywanie chronionych danych również do portali, w przypadku których dane wysyłane są dzielone na fragmenty, co normalnie uniemożliwia ich właściwą analizę.
 | 1 pkt |  |
| 1. System musi umożliwiać blokowanie wykonywania zrzutów ekranu (print screen) na stacji końcowej, co w połączeniu z funkcją OCR dla danych przesyłanych w sieci (patrz **punkt 45**) powinno znacznie utrudnić możliwość wykonania zrzutu ekranu i przesłania chronionych treści w postaci grafiki.
 | 1 pkt |  |
| 1. System musi umożliwiać instalację agenta na komputerach z systemem Mac OS X oraz macOS

(Dopuszcza się, że nie wszystkie funkcje wymienione w **punkcie 14 oraz 46** są dostępne na wszystkich systemach operacyjnych z zastrzeżeniem, iż dla Mac OS X musi być dostępna większość funkcji w szczególności: lokalnego wykrywania, kontroli aplikacji oraz monitorowania ruchu web i e-mail.) | 1 pkt |  |
| 1. Ochrona wdrożona w postaci agenta systemu DLP na komputerze użytkownika musi umożliwiać detekcję z użyciem wszystkich zdefiniowanych w systemie mechanizmów identyfikacji danych wliczając w to fingerprinty dla danych ustrukturyzowanych z baz danych (patrz **punkt 38.a.**).
 | 1 pkt |  |
| 1. System musi wykrywać próby wysyłania danych nie tylko w dużych paczkach, ale również w mniejszych partiach, np. po kilka rekordów z bazy danych. W tym celu system musi umożliwiać kumulowanie informacji o transmisjach chronionych informacji, nawet gdy poszczególne transmisje nie spełniają zdefiniowanego w regułach progu, ale sumarycznie go przekraczają. Po spełnieniu określonego w regule warunku w systemie powinien powstać incydent naruszenia polityk DLP ze wskazaniem szczegółów incydentu oraz dodatkowo informacji, kiedy miała miejsce pierwsze i ostatnie naruszenie związane z sumarycznym spełnieniem warunku reguły DLP.
 | 1 pkt |  |
| 1. System musi umożliwiać integrację z usługami katalogowymi w celu m.in.:
 |
| * 1. przypisania użytkowników i grup jako autoryzowanych nadawców i odbiorców chronionych informacji,
 | 1 pkt |  |
| * 1. przypisania użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,
 | 1 pkt |  |
| * 1. wyświetlenia szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o przełożonym oraz departamencie użytkownika.
 | 1 pkt |  |
| * 1. automatycznego wysłania powiadomienia do przełożonego (menadżera) osoby będącej źródłem incydentu w przypadku jego wystąpienia.
 | 1 pkt |  |
| 1. System musi umożliwiać wykrywanie danych w następujących zasobach w sieci Zamawiającego:
 |
| * 1. Bazy danych
 | 1 pkt |  |
| * 1. Pliki Outlook PST
 | 1 pkt |  |
| 1. W przypadku wykrycia plików, których nie powinno być w danym miejscu oprócz stworzenia incydentu powinno być możliwe automatyczne zareagowanie przez system DLP np. usunięcie pliku i stworzenie w nim innego pliku z informacją dla użytkownika.
 | 1 pkt |  |
| 1. W przypadku, gdy System działa w integracji z wspieranymi systemami klasyfikacji informacji, musi umożliwiać nadawanie etykiety klasyfikacji dla pliku spełniającego kryteria zdefiniowane w zadaniu wykrywania danych na komputerach użytkowników.
 | 1 pkt |  |
| 1. Dostęp do konsoli zarządzającej musi wymagać uwierzytelnienia. Oprócz hasła systemu DLP oraz hasła użytkownika z usługi katalogowej system DLP musi wspierać silne uwierzytelnianie cyfrowym certyfikatem użytkownika oraz integrację z systemem silnego uwierzytelniania opartego o hasło jednorazowe (ang. One Time Password) przynajmniej jednego producenta.
 | 1 pkt |  |
| 1. System DLP w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana (dane forensic). Wgląd w tak szczegółowe informacje powinien być kontrolowany zgodnie z **pkt. 23**.
 | 1 pkt |  |
| 1. Konsola zarządzająca musi umożliwiać zarządzanie i pracę nad incydentami, m.in.
 |
| * 1. zmianę statusu incydentu (nowy, przetwarzany, zamknięty), przy czym musi istnieć możliwość tworzenia własnych statusów,
 | 1 pkt |  |
| * 1. zmianę ważności incydentu (niska, średnia, wysoka),
 | 1 pkt |  |
| * 1. dodanie komentarza do incydentu,
 | 1 pkt |  |
| * 1. dodanie etykiety (Tag) do incydentu,
 | 1 pkt |  |
| * 1. oznaczenie incydentu jako ignorowany,
 | 1 pkt |  |
| * 1. przypisanie incydentu do administratora systemu DLP,
 | 1 pkt |  |
| * 1. przekazywanie incydentu do innego administratora systemu DLP (eskalacja),
 | 1 pkt |  |
| * 1. usunięcie incydentu, przy czym usunięciu incydentu musi towarzyszyć automatyczne odnotowanie tej operacji w logu audytowym oraz opcjonalne wysłanie powiadomienia do administratora systemu DLP.
 | 1 pkt |  |
| 1. Zarządzanie incydentami musi być możliwie na co najmniej dwa sposoby:
	1. Uprzywilejowana osoba (administrator systemu DLP, analityk incydentów) loguje się do konsoli zarządzania systemu DLP, odnajduje odpowiedni incydent i wykonuje na nim odpowiednie akcje.
	2. System DLP wysyła automatyczne powiadomienie dotyczące naruszenia polityki DLP do wyznaczonej osoby (administrator systemu DLP, analityk incydentów). Powiadomienie zawiera szczegóły incydentu oraz odnośniki pozwalające na zarządzanie nim, dzięki czemu podejmowanie działań względem incydentu nie wymaga od tej osoby logowania się do konsoli zarządzania systemu DLP.
 | 3 pkt |  |
| 1. System musi udostępniać REST API umożliwiające dostęp do incydentów oraz zarządzanie nimi z poziomu aplikacji i systemów firm trzecich. API musi wykorzystywać mechanizmy bezpieczeństwa w oparciu o JSON Web Token (JWT).
 | 1 pkt |  |
| 1. Konsola zarządzania musi zawierać sekcję pozwalającą administratorom na monitorowanie i ocenę poprawności działania systemu jak i obciążenia poszczególnych modułów systemu DLP.
 | 1 pkt |  |
| 1. System DLP musi dostarczać mechanizmy wspomagające pracę administratorów poprzez wykorzystanie cyklicznej automatycznej analizy incydentów pod kątem ryzyka stanowionego dla organizacji i prezentowania tak rozpoznanych zagrożeń w sposób pogrupowany i uporządkowany począwszy od zagrożeń najbardziej istotnych.
 | 1 pkt |  |
| 1. W odniesieniu do **poprzedniego punktu** system DLP powinien klasyfikować rozpoznane zagrożenia do kilku kategorii np. potencjalna kradzież danych, czy nieprawidłowy proces biznesowy.
 | 1 pkt |  |
| 1. Ze względu na różne role pełnione przez pracowników Zamawiającego system musi umożliwić nadawanie odpowiednich kategorii pracownikom np. pracownik wysokiego ryzyka, czy pracownik uprzywilejowany, które to kategorie będą odpowiednio uwzględniane przez mechanizm opisany **w dwóch wcześniejszych punktach**.
 | 1 pkt |  |
| 1. Rozwiązanie musi współpracować poprzez protokół ICAP ([RFC](https://en.wikipedia.org/wiki/RFC_%28identifier%29) [3507](https://datatracker.ietf.org/doc/html/rfc3507)) z dowolnym serwerem proxy i cache, umożliwiając inspekcję połączeń HTTP(S) i analizę informacji wysyłanych tym kanałem w celu sprawdzenia zgodności z polityką ochrony informacji systemu DLP
 | 1 pkt |  |
| Suma | **69 pkt** |  |