

Opis Przedmiotu Zamówienia

Zaprojektowanie i wdrożenie rozwiązania DLP

Spis treści

1.	Przedmiot zamówienia	3
2.	Zakres prac	4
3.	Wymagania funkcjonalne	6
4.	Wymagania нефункционалне	7
5.	Integracje wymagane	8
6.	Metodyka wdrożenia i etapowanie	9
7.	Kryteria odbioru	10
8.	Utrzymanie i wsparcie	11
9.	Postanowienia ogólne	12

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zaprojektowanie i wdrożenie systemu Data Loss Prevention (DLP), mającego na celu ograniczenie ryzyka wycieku danych oraz zapewnienie egzekwowania polityk ochrony informacji w kanałach: endpoint, poczta, WWW, aplikacje chmurowe, współdzielenie plików i nośniki zewnętrzne.

System DLP musi być dostarczony w modelu chmurowym SaaS. Konsola zarządzająca rozwiązaniem DLP powinna być zlokalizowana w centrum danych na terenie UE/EOG, w celu zapewnienia zgodności z przepisami o ochronie danych osobowych (RODO/GDPR) oraz wymogami rezydencji danych Zamawiającego.

Po stronie Zamawiającego wymagane jest jedynie wdrożenie agentów na urządzeniach końcowych

Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych, spełniających wymagania funkcjonalne i нефункционалне określone w OPZ.

Wszelkie odniesienia do standardów, technologii, mechanizmów klasyfikacji lub integracji należy rozumieć jako „lub równoważne”, zgodnie z art. 99 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z późn. zm.).

Zamawiający wymaga, aby licencja na zaproponowane rozwiązanie obejmowała okres: 36 miesięcy od daty wdrożenia.

Lp.	Nazwa	Liczba sztuk
1	Zaprojektowanie i dostarczenie rozwiązania wraz z niezbędnymi licencjami	1
2	Usługa wdrożenia oraz szklenia	1

2. Zakres prac

Etap	Zakres / produkt	Minimalna zawartość
Analiza przedwdrożeniowa	Raport analizy i koncepcja DLP	Inwentaryzacja kanałów exfiltracji, mapowanie danych, analiza ryzyk, wymagania integracyjne, Ocena środowiska klienta pod kątem przepływu danych wrażliwych, identyfikacja źródeł danych (endpointy, chmura, e-mail), klasyfikacja informacji oraz określenie wymagań regulacyjnych (np. RODO, DORA)
Projekt techniczny	Projekt architektury DLP	Architektura logiczna i fizyczna, przepływy danych, integracje (IdP/AD, SIEM, MDM, poczta, chmura), wymagania sieciowe i porty, model uprawnień. Opracowanie architektury wdrożenia FortiDLP obejmującej komponenty (Endpoint Agent, Network/Cloud), integracje (np. z AD, SIEM, CASB), sposób komunikacji oraz wysoką dostępność.
Polityki DLP	Katalog polityk + macierz reguł	Konfiguracja polityk DLP (do 10 polityk) Wykorzystanie wbudowanych detektorów: <ul style="list-style-type: none"> • Numery kart płatniczych • Dane finansowe • Wzorce niestandardowe (3 przykładowe w oparciu o REGEX)
Konfiguracja i wdrożenie	Uruchomienie produkcyjne	<ol style="list-style-type: none"> Integracja z katalogiem użytkowników <ul style="list-style-type: none"> • Integracja z Azure AD • Synchronizacja użytkowników i grup • Mapowanie polityk do grup Konfiguracja polityk DLP (do 10 polityk) Wykorzystanie wbudowanych detektorów: <ul style="list-style-type: none"> • Numery kart płatniczych • Dane finansowe • Wzorce niestandardowe (3 przykładowe w oparciu o REGEX) Przykładowe polityki: <ul style="list-style-type: none"> • Kopiowanie danych wrażliwych na USB → monitor + alert • Upload do aplikacji chmurowych → monitor • Wklejanie danych do przeglądarki → alert Przygotowanie agenta endpoint <ul style="list-style-type: none"> • Pobranie paczki instalacyjnej z portalu • Konfiguracja instalatora • Test na 10 wybranych stacjach • Weryfikacja komunikacji agent–chmura Konfiguracja reakcji i workflow <ul style="list-style-type: none"> • Alert e-mail do SOC / IT • Dashboard incydentów • Ustawienie poziomów ryzyka • Konfiguracja user notification (komunikat dla użytkownika)
Testy	Plan testów + protokoły	Testy funkcjonalne <ul style="list-style-type: none"> • Kopiowanie pliku z PESEL na USB • Upload dokumentu do OneDrive / Google Drive • Weryfikacja logów i alertów

Szkolenia	Szkolenia i materiały	<p>Szkolenie administratorów - 3 os. (min. 16g) w formie zdalnej lub on site</p> <ul style="list-style-type: none"> • Przegląd konsoli • Analiza incydentów • Tworzenie nowych polityk • Raportowanie • Eksport danych • Dobre praktyki strojenia (tuning false positives)
Dokumentacja	Dokumentacja powdrożeniowa	Instrukcje administracyjne, runbooki, procedury wyjątków, procedury reagowania, opis konfiguracji i kopii zapasowych.
Stabilizacja	Okres stabilizacji	Wsparcie po uruchomieniu, obejmujące strojenie polityk (tuning), redukcję false positives oraz przygotowanie końcowego raportu stabilizacji, realizowane będzie przez okres 36 miesięcy w ramach puli 48 godzin

3. Wymagania funkcjonalne

Obszar funkcjonalny	Wymaganie
Ochrona kanałów	System musi wspierać egzekwowanie polityk DLP co najmniej dla: endpoint (stacje/serwery), poczta, przeglądarka/WWW, współdzielenie plików, aplikacje chmurowe (SaaS) oraz nośniki wymienne (USB). System musi wspierać dodatkowo: <ul style="list-style-type: none"> - schowek systemowy - Bluetooth/AirDrop - drukowanie - zrzuty ekranu - CLI - Shadow AI w zakresie oferowanym przez rozwiązanie.
Detekcja danych	Wykrywanie danych na podstawie: wyrażeń regularnych, słowników, algorytmów walidacji (np. sumy kontrolne), identyfikatorów i wzorców dokumentów.
Zgodność z dobrymi praktykami	System powinien wspierać klasyfikację opartą o kontekst i treść, w tym możliwość użycia klasyfikatorów statystycznych/ML oraz dopasowania „fingerprinting”
Klasyfikacja i etykietowanie	Obsługa etykiet/klasyfikacji informacji i ich egzekwowania w politykach (np. „Publiczne/Wewnętrzne/Poufne/Ścisłe poufne”). Możliwość automatycznego i ręcznego oznaczania.
Reakcje/polityki	Co najmniej: monitorowanie, ostrzeganie użytkownika (user coaching), blokowanie, kwarantanna, wymuszenie szyfrowania, przekierowanie do zatwierdzenia, zgłoszenie incydentu. System powinien umożliwiać również: <ul style="list-style-type: none"> - zapis kopii pliku w celach dowodowych - przechwycenie schowka - wykonanie zrzutu ekranu w momencie incydentu - izolację/blokowanie urządzenia końcowego w przypadkach wysokiego ryzyka, jeżeli funkcjonalność jest dostępna w oferowanym rozwiązaniu - zamykanie procesów wysokiego ryzyka System musi wspierać mechanizmy interakcji z użytkownikiem w punkcie dostępu do danych, w tym komunikaty edukacyjne zwiększające świadomość bezpieczeństwa.
Obsługa wyjątków	Mechanizm wyjątków z workflow akceptacji (czasowe/stałe), z audytem kto i kiedy zatwierdził oraz uzasadnieniem.
Ochrona endpoint	Kontrola: kopiowania do schowka, drukowania, zrzutów ekranu (jeśli technicznie możliwe), kopiowania na USB, przesyłania przez aplikacje komunikacyjne (w zakresie obsługiwanym), uploadu do usług współdzielenia plików.
Poczta	Kontrola wiadomości wychodzących i załączników, możliwość działań: blokuj/kwarantanna/uzasadnienie/ostrzeżenie; wsparcie dla szyfrowania i kontroli adresatów (np. domeny zewnętrzne).
Chmura i współdzielenie plików	Monitorowanie i egzekwowanie polityk dla udostępnień, linków publicznych, współdzielenia zewnętrznego, uprawnień, oraz przesyłania danych do aplikacji SaaS.
Raportowanie i analityka	Dashboardy: trendy, kanały, typy danych, użytkownicy, lokalizacje. Eksport raportów. Raporty dla audytu i zgodności.
Integracja incydentowa	Integracja z procesem obsługi incydentów: generowanie zdarzeń, korelacja, nadawanie priorytetu, możliwość przekazania do systemu SIEM/SOAR/ticketing (zgodnie z posiadanymi narzędziami Zamawiającego).
API / automatyzacja	Udokumentowany interfejs (API) do pobierania zdarzeń, zarządzania wyjątkami lub integracji z workflow (jeśli dostępne w rozwiązaniu).
Analiza incydentów	System powinien mapować działania wysokiego ryzyka do bazy MITRE Engenuity lub równoważnych standardów klasyfikacji TTP.

4. Wymagania niefunkcjonalne

Obszar	Wymaganie
Skalowalność	Możliwość obsługi wskazanej liczby użytkowników/urządzeń bez degradacji kluczowych funkcji. Liczba użytkowników: 120.
Wysoka dostępność	Jeśli wdrożenie obejmuje komponenty lokalne: wymagana architektura dla elementów krytycznych lub przedstawienie równoważnego mechanizmu ciągłości działania.
Bezpieczeństwo	Szyfrowanie danych w tranzycie i w spoczynku, kontrola dostępu oparta o role (RBAC), MFA poprzez integrację z IdP. Wymagania bezpieczeństwa wynikają z konieczności zapewnienia zgodności z przepisami RODO (UE 2016/679), ustawą o krajowym systemie cyberbezpieczeństwa oraz dobrymi praktykami ochrony informacji.
Minimalizacja danych	Logi i dane telemetryczne mają być adekwatne do celów bezpieczeństwa; możliwość maskowania/anonimizacji fragmentów treści w logach. Rozwiązanie musi jasno wskazywać, jakie dane telemetryczne są wysyłane do chmury producenta, musi umożliwiać pseudonimizację danych w wybranym zakresie. Dane muszą być przesyłane w sposób minimalizujący koszty i wymagania przepustowości
Wydajność endpoint	Agent nie może w sposób istotny obniżać wydajności stacji roboczych; Wykonawca przedstawi rekomendacje i metryki monitorowania.
Zarządzanie zmianą	Zmiany polityk: wersjonowanie, możliwość szybkiego rollbacku, środowisko testowe/pilotażowe lub tryb „symulacji/monitor-only”.
Zgodność i audyt	Pełny audyt działań administracyjnych, zmian polityk oraz wyjątków; retencja logów zgodna z wymaganiami Zamawiającego.
Język i użyteczność	Konsola administracyjna i komunikaty dla użytkownika w języku polskim lub angielskim, możliwość dostosowania treści komunikatów.
Reakcje	Zapis kopii pliku oraz zawartości schowka powinien być możliwy w lokalizacji wskazanej przez Zamawiającego poza infrastrukturą producenta. Mechanizmy rejestracji zdarzeń (np. kopie dowodowe, przechwycenie schowka, zrzuty ekranu) muszą być stosowane wyłącznie w zakresie niezbędnym do zapewnienia bezpieczeństwa informacji, zgodnie z RODO oraz przepisami prawa pracy dotyczącymi monitoringu (art. 22 ² –22 ³).

5. Integracje wymagane

Integracja	Wymaganie
Tożsamość	Integracja z usługą katalogową/IdP (np. AD/LDAP lub równoważne) dla identyfikacji użytkowników i grup oraz przypisywania polityk.
Komunikacja	Możliwość powiadomień o incydentach przez Microsoft Teams oraz Slack.
SIEM	Eksport zdarzeń do systemu klasy SIEM w formacie uzgodnionym (syslog/API/connector), wraz z mapowaniem pól i priorytetów.
Klasyfikacja	Wsparcie dla Microsoft Sensitivity Labels.
Ticketing/ITSM	Opcjonalnie: automatyczne tworzenie zgłoszeń incydentów DLP w narzędziu ITSM, z atrybutami: użytkownik, kanał, typ danych, podgląd/odniesienie, rekomendowana akcja.
MDM/UEM	Jeżeli Zamawiający posiada, integracja z systemem zarządzania urządzeniami w zakresie dystrybucji agentów/polityk lub tagowania urządzeń.
Poczta i współpraca	Integracja z posiadanym systemem poczty i narzędziami współpracy/pliki (on-prem lub chmurowe) w zakresie polityk DLP.

6. Metodyka wdrożenia i etapowanie

Faza	Wymaganie
Pilotaż	Wdrożenie pilotażowe na ograniczonej grupie użytkowników i wybranych kanałach, w trybie monitorowania + user coaching.
Strojenie	Iteracyjne dostrajanie reguł w celu minimalizacji false positives; dokumentacja wyjątków i decyzji.
Produkcja etapami	Stopniowe rozszerzanie zakresu (kanały, jednostki, typy danych) oraz przełączanie polityk z „monitor” do „blokuj” dla uzgodnionych przypadków.
Komunikacja do użytkowników	Przygotowanie komunikatów i zasad: dlaczego blokuje, jak zgłosić wyjątek, jak bezpiecznie udostępniać dane.
Transfer wiedzy	Warsztaty operacyjne: tworzenie reguł, analiza zdarzeń, obsługa wyjątków, procedury utrzymania.

7. Kryteria odbioru

Obszar	Kryterium odbioru
Uruchomienie	System działa produkcyjnie w uzgodnionym zakresie kanałów i grup użytkowników. Uruchomienie polityk obejmujących min. USB, schowek, SaaS oraz pocztę Web. Dostępny widok aktywności użytkownika „przed/w trakcie/po incydencie”.
Polityki	Dostarczony i wdrożony katalog polityk (min. 10 reguł uzgodnionych w analizie), w tym polityki dla danych osobowych i dokumentów poufnych.
Testy	Pozytywnie zakończone testy scenariuszy: wysyłka mail z danymi wrażliwymi, upload do chmury, kopiowanie na USB, udostępnienie linkiem zewnętrznym (w zależności od zakresu).
Raporty	Dostępne dashboardy i raporty okresowe; możliwość eksportu i integracji z SIEM.
Dokumentacja i szkolenia	Przekazana dokumentacja powdrożeniowa + przeprowadzone szkolenia; protokoły i materiały szkoleniowe.
Stabilizacja	Zakończony okres stabilizacji, raport z listą wprowadzonych korekt i rekomendacji dalszego rozwoju.

8. Utrzymanie i wsparcie

Obszar	Wymaganie OPZ
Wsparcie wykonawcy	Wsparcie powdrożeniowe przez min. 36 miesięcy od daty wdrożenia.
Wsparcie producenta	Wykonawca zapewni 12 miesięczną subskrypcję eksperckiego wsparcia technicznego producenta systemu DLP, obejmującą m.in. okresowe przeglądy konfiguracji wdrożonego rozwiązania, tuning wydajności, rekomendacje integracyjne oraz identyfikację obszarów wymagających usprawnień operacyjnych.
Rozwój polityk	Pakiet godzin na kwartalne przeglądy polityk DLP, rekomendacje usprawnień i aktualizacje reguł.
Aktualizacje	Wykonawca zapewni plan aktualizacji komponentów oraz testy regresji polityk po aktualizacjach.
Certyfikaty	Zamawiający wymaga, aby Wykonawca posiada certyfikaty ISO 27001, ISO 9001 lub równoważne.

9. Postanowienia ogólne

Zamawiający dopuszcza rozwiązania równoważne spełniające wymagania OPZ.

Wymagania dotyczące bezpieczeństwa, rezydencji danych oraz przetwarzania informacji wynikają z obowiązujących przepisów prawa, w szczególności RODO (UE 2016/679) oraz ustawy Prawo zamówień publicznych.

Szczegółowe mechanizmy kontroli użytkowników muszą być wdrażane zgodnie z zasadą minimalizacji oraz adekwatności.