FORMULARZ INFORMACYJNY DLA MOŻLIWOŚCI WSPÓŁPRACY Z KGHM POLSKA MIEDŹ S.A.

Dialog techniczny / badanie rynku dotyczące wdrożenia systemu klasy DLP w organizacji mający na celu selekcje rozwiązań spełniających wymagania organizacji

KGHM Polska Miedź S.A.
Oddział COPI
ul. M. Skłodowskiej-Curie 45b
59-301 Lubin

W związku z zaproszeniem do złożenia formularza informacyjnego działając w imieniu na rzecz (nazwa firmy)

……..……..…

…… ……

składamy przedmiotowy formularz,

I. Dane dotyczące firmy:

1.	Nazwa firmy:	
2.	Adres firmy:	
3.	Telefon kontaktowy:	
4.	Nr faksu:	
5.	E-mail:	
6.	NIP:	
7.	REGON:	
8.	Dane kontaktowe inspektora ochrony danych osobowych (e-mail lub nr telefonu)	
9.	Imię i Nazwisko (nr telefonu) osoby(ób) odpowiedzialnej(ych) ze strony Wykonawcy za realizację zadania.	

II. Warunki handlowe oferty:

1. **Ogólne warunki:**

Na podstawie poniższego formularza informacyjnego, proszę o przygotowanie *wstępnej oferty handlowej*. Formularz proszę uzupełnić i dołączyć do projektu RFI w Systemie SAP ARIBA. Załącznikiem do formularza jest arkusz oceny, który każdy z uczestników RFI musi uzupełnić zgodnie z przedstawionymi kryteriami. Dopuszczamy możliwość odesłania dokumentacji również pocztą elektroniczną. **Termin do 21.11.2025 r. do godziny 13.00.**

2. **Przedmiot zapytania**

Organizacja docelowo jest zainteresowana wdrożeniem systemu klasy DLP w KGHM i Spółkach Grupy Kapitałowej

- Liczba użytkowników objętych systemem 10000-12000 (inicjalna wartość), w celu kalkulacji cenowej proszę przyjąć 12000
- System musi być zdolny do pracy w organizacjach rozproszonych geograficznie (oddziały w PL i zagranicą).
- Wsparcie architektury multi-tenant

- Instalacja i konfiguracja w infrastrukturze zamawiającego (środowisko on-premise - Wymóg wsparcia architektury hybrydowej on-premise + cloud)
- Integracja z środowiskami M365 wykorzystywanymi przez zamawiającego
- Wsparcie dla systemu przez okres 36 miesięcy (wsparcie techniczne 24/7 w języku polskim lub angielskim)
- System musi pracować z dokumentami w języku Polskim, Angielskim i Hiszpańskim (opcjonalnie)
- Utrzymanie cen dla zakupu dodatkowych licencji/subskrypcji w okresie 36 miesięcy
- Możliwość objęcia systemem (albo możliwość wykreowania dodatkowych instancji) systemów znajdujących się w spółkach grupy kapitałowych w Polsce i zagranicą – nie więcej niż 3 instancje (KGHM P.M. S.A., KGHM International, Grupa Kapitałowa KGHM)
- Pole eksploatacji KGHM i spółki GK , które obsługuje KGHM pod względem IT , w tym spółki zagraniczne
- System musi mieć możliwość pracy z różnymi domenami w jednym lesie jak i w różnych lasach Active Directory
- System musi pracować z różnymi tenantami środowiska M365 w konfiguracji hybrydowej
- System musi posiadać realizowalny Plan Wyjścia z rozwiązania (Jasno zdefiniowana procedura migracji do innego dostawcy)
- Możliwość integracji z Active Directory i AAD dla automatycznego zarządzania tożsamościami.
- Wymagane SLA wydajnościowe – np. czas klasyfikacji pliku < 3 sekundy.

- Wymóg dostarczenia mechanizmów eksportu polityk, logów i konfiguracji w formatach otwartych (XML, JSON, CSV).

- System musi wspierać logowanie do centralnego SIEM

- Musi być dostępny portal self-service dla użytkowników (np. wnioski o wyjątek, podgląd klasyfikacji dokumentu).

- Możliwość obsługi nie tylko środowiska on-premise ale także SaaS czy Cloud

3. Funkcjonalności będące przedmiotem zainteresowania :

3.1. Wymagania funkcjonalne systemu klasy DLP w zakresie ochrony danych:

1. Zaawansowana klasyfikacja danych (zwana etykietowaniem czy tagowaniem plików):
    a. Klasyfikacja automatyczna (np. po treści dokumentu, źródle jego pochodzenia),
    b. Klasyfikacja ręczna przez użytkownika,
    c. Klasyfikacja dziedziczona - związana z kopiowaną treścią z dokumentu źródłowego,
    d. Klasyfikacja dokumentu nie może być obniżona bez odnotowania tego faktu w logach audytowych w systemie,
    e. Obniżenie klasyfikacji pliku możliwe dla wybranej grupy użytkowników wraz z możliwością przedstawienia raportu zawierającego wykaz obniżonej klasyfikacji,
    f. Możliwość wygenerowania wyjątku na żądanie dla ustalonej grupy użytkowników w celu ominięcia reguł (np. pilne uzasadnione przesłanie mailem pliku o kategorii wewnętrzne) – w obsłudze wyjątku przez użytkownika należy odnotować potrzebę takiej czynności wraz z możliwością przedstawienia raportu zawierającego wykaz obniżonej klasyfikacji,
    g. Klasyfikacja plików niezależnie od typu/rodzaju pliku (wszystkie typy plików).
    h. Możliwość ręcznego kształtowania słownika etykiet przez określoną grupę użytkowników.

2. Zarządzanie regułami/politykami ochrony informacji :
    a. System posiada wbudowane wzorce reguł dla ochrony informacji regulowanej prawem lub dobrymi praktykami,
    b. Możliwość ustalania własnych reguł ochrony danych uzależnionych od cech chronionych informacji (np. klasyfikacja, typ pliku, użytkownik, kanał transmisji, treść, fingerprint itp.),
    c. Możliwość uruchomienia reguły na wybranej grupie użytkowników,
    d. Uruchomienie dowolnej reguły wykorzystującej :
        - wzorce tekstowe (Regex)
        - wzorce wyliczeniowe
        - słowniki
        - typy plików.

    Możliwość uruchomienia w regułach skryptów zewnętrznych.
3. Logowanie zdarzeń naruszenia zasad przetwarzania danych osobowych,
    a w szczególności :
    a. Czas naruszenia,
    b. Dane użytkownika oraz osób uczestniczących,
    c. Rodzaj naruszonej reguły,
    d. Rodzaj naruszenia i zebranie artefaktów takiego zdarzenia w celu pełnego jego obrazu,
    e. Wskazanie miejsca dopasowania danych do reguły (przyczynę wyzwolenia incydentu),
    f. Informacje o urządzeniu,
    g. Dane sieciowe,
    h. Działania podjęte przez system.

4. Obsługa incydentów przez zdefiniowanych użytkowników systemu:
    a. Generowanie automatycznych raportów z działań związanych z obsługą incydentów,
    b. Podział procesu obsługi incydentów na poszczególne grupy użytkowników,
    c. Możliwość ograniczenia dostępu do artefaktów incydentu w zależności od przypisanej roli,
    d. Klasyfikacja incydentów,
    e. Grupowanie incydentów,
    f. Masowa obsługa incydentów,
    g. Filtrowanie zdarzeń w zależności od potrzeb użytkownika (możliwość ustawień filtrów w sposób spersonalizowany).

5. Kanały ochrony danych:

    a. Zasoby plikowe SMB/CIFS (w tym obsługa ADS),
    b. Drukowanie dokumentów,
    c. Poczta elektroniczna,
    d. Komunikatory,
    e. Web - Aplikacje webowe (np. webmaile, WebDAV, formularze),
    f. Virtual Desktop,
    g. EndPointy,
    h. Zrzut ekranu – przy wyświetleniu plików z określonej w konfiguracji kategorii.

6. OCR – Możliwość aplikacji do rozpoznawania obrazów w celu znalezienia danych chronionych. Funkcjonalność powinna być możliwa do wdrożenia we wszystkich kanałach ochrony danych.

7. Discovery – przeszukanie danych w spoczynku w celu odnalezienia informacji podlegającej ochronie i automatycznie przypisanie kategorii:
    a. File serwery,
    b. Bazy danych,
    c. Sharepoint,
    d. Exchange Serwer i Endpoint,
    e. Możliwość ustawienia reguł automatycznych.

8. Zarządzanie urządzeniami pamięci masowej USB:
    a. Zarzadzanie poprzez białą listę nośników,
    b. Blokowanie nieautoryzowanych urządzeń,
    c. Pełne monitorowanie aktywności, w tym logowanie zdarzeń prób kopiowania danych na nośniki nieautoryzowane oraz ewidencja kopiowanych danych na dopuszczone nośniki. Generowanie określonych rodzajów raportów automatycznie i przekazywanie jednostkom odpowiedzialnym za nadzór przez workflow.

9. Szyfrowanie danych:
    a. Możliwość automatycznego szyfrowania danych w zależności od ustawień polityki ochrony informacji (np. automatyczne szyfrowanie nośnika USB lub plików w momencie kopiowania danych o określonych etykietach),
    b. Szyfrowanie załączników w zależności od klasyfikacji załączników.

10. Machine Learning:
    a. Możliwość wgrania wzorców firmowych dokumentów (np. FV, Umowy)
    b. Fingerprinting dokumentu.

11. Kontrola przekazanych danych poza infrastrukturą KGHM:
    a. Kontrola dostępu do pliku per użytkownik wraz ze zbieraniem artefaktów tego zdarzania,

   b. Możliwość ustalenia terminu dostępności pliku po którym plik nie zostanie otworzony,
   c. Blokada dostępu do pliku na żądanie (odwołanie przyznanych praw w trybie natychmiastowym),
   d. Kontrola użytkowników zewnętrznych po stronie systemu DLP,
   e. Logowanie prób nieautoryzowanego dostępu – zebranie artefaktów w celu udokumentowania zdarzenia w tym (pochodzenie pliku),
   f. Zdefiniowanie określonych rodzajów danych, które z uwagi na swoją krytyczność nie mogą być udostępniane poza infrastrukturę KGHM.

12. User Behaviour Analiser:
    Wykrycie zachowania użytkowników odbiegających od zachowania standardowego mogącego świadczyć o wycieku informacji.

3.2. Wymagania funkcjonalne systemu klasy DLP w zakresie działania systemu:

1. Kontrola dostępu do systemu i danych oparta na rolach (RBAC),

2. Skanowanie danych w czasie rzeczywistym,

3. Niezaprzeczalność wystąpienia incydentu – zbiór artefaktów z dowodami naruszenia,

4. Rozliczalność czynności użytkowników systemu DLP - logi obejmują wszystkie czynności z przeglądu artefaktów poszczególnych incydentów,

5. Brak możliwości usunięcia/ingerencji w logi ze zdarzeń:
   a. Funkcjonalnych,
   b. Administracyjnych.

6. Możliwość współpracy z Office365,

7. Integracja z systemami bezpieczeństwa :
   a. SIEM,
   b. IPS/IDS.

8. Możliwość kształtowania własnych opisów alertów po stronie użytkownika,

9. Zgłaszanie nietypowych wzorców zachowania na danych (kopiowanie dużej ilości danych, poza określonymi godzinami itp.,

10. Generowanie określonych raportów wg. wskazanego zapotrzebowania.

11. Predefiniowane raporty z możliwością dostosowania do potrzeb organizacji

4. Kryteria:

Przy założeniu spełnienia wymagań wyspecyfikowanych w punkcie pierwszym, do dalszych rozmów zostaną zaproszeni oferenci rozwiązań które na podstawie załączonego arkusza uzyskają minimum 65 punktów na 98 możliwych do zdobycia uwzględniając kompletność danych w nim zawartych. W przypadku braku spełnienia tego warunku, przez co najmniej 4 rozwiązania do dalszych rozmów zostaną dopuszczone 4 najlepsze technologie według uzyskanego rankingu.

Istotne elementy dla organizacji w ujęciu ogólnym :

- Spełnienie funkcjonalności wymienionych we wcześniejszym punkcie zgodnie z załączonym arkuszem kalkulacyjnym, przy założeniu spełnienia wymagań niezbędnych określonych w punkcie pierwszym.

- Kompletność danych w arkuszu.

- Całościowe koszty dla budowanego systemu w okresie 60 miesięcy liczony od daty podpisania przez Strony protokołu końcowego odbioru uwzględniające

    - Koszty subskrypcji lub licencji i maintenance'u oprogramowania
    - Koszty Usługi bieżącego wsparcia oprogramowania -
    - Koszty Usługi wsparcia rozszerzonego - 230h rocznie
    - Koszty licencji/subskrypcji oprogramowania trzeciego niezbędnego do świadczenia usługi (np.. Bazy danych, systemy operacyjne wirtualizatory, wtyczki po cennikach producenckich – bez upustów)
    - Koszty związane z zakupem potrzebnego sprzętu do uruchomienia systemu po cennikach producenckich
    - Koszt wdrożenia plus szkoleń

- Możliwość zaadresowania maksymalnie dużego obszaru infrastruktury z wykorzystaniem istniejących już narzędzi

- Efektywne wykorzystanie narzędzi posiadanych już w środowisku zamawiającego (DLP M365)

- Możliwość obsługi nie tylko środowiska on-premise ale także SaaS czy Cloud

5. Warunki udziału:

- Udokumentowane co najmniej 2 wdrożenia wdrożenia w środowiskach o podobnej wielkości oraz specyfiki rodzaju przetwarzanych informacji

- Potwierdzone kompetencje w zakresie wdrażanego produktów (referencje , certyfikaty)

- Wskazane jest aby rozwiązanie było obecne na liście Gartnera lub musi pochodzić od producenta który jest uznaną marką w zakresie weryfikowanego obszaru technologicznego

- Oferent musi być autoryzowanym partnerem producenta rozwiązania bądź producentem rozwiązania

- Gotowość do certyfikacji zgodnie z wymaganiami ustawy o KSC

- **Oferent wyraża zgodę na prezentacje oferowanego rozwiązania w zakresie spełnienia wymagań wyspecyfikowanych przez zamawiającego w środowisku demo lub jako POC w środowisku zamawiającego jak również implementacji szczególnych przypadków użycia jeśli zamawiający takie wskaże.**

- W przypadku konieczności przekazania dodatkowych danych związanych ze stosowaną technologią w organizacji przez zamawiającego oferent wyraża zgodę na podpisanie dokumentu o zaufaniu poufności (NDA).

6. Harmonogram :

- Etap 1 - Preselekcja rozwiązań do 15.12.2025
- Etap 2 - Szczegółowa weryfikacja wymagań przez zamawiającego do do 30.06.2026 i ich zakwalifikowanie do potencjalnego postępowania zakupowego

W związku z trybem prowadzonego projektu – dialog techniczny / badanie rynku, Zamawiający umożliwia spotkania on-line z zainteresowanymi uczestnikami, rozmowy telefoniczne oraz pytania i odpowiedzi. Prosimy pamiętać, że konsultacje mogą odbyć się przed upływem terminu RFI tj. przed dniem 21.11.2025r. godz. 13:00

3. Warunki cenowe

Zgodnie z Formularzem pomocniczym – arkuszem oceny stanowiącym załącznik do niniejszego dokumentu.

4. Warunki umowne

Zamawiający udostępnia w RFI przykładowy projekt umowy, który jest zawierany w ramach postepowań przetargowych z Oferentami. Dostępne w nim zapisy formalne w tym korporacyjne co do zasady są nienegocjowane. O finalnej treści dokumentu zadecyduje wynik prowadzonego RFI i zostanie uwzględniony przy potencjalnym właściwym postępowaniu zakupowym.

5. Zarządzanie jakością

Czy Państwa firma posiada certyfikaty? TAK / NIE*

Jeśli tak to jakie:

……...

Jeśli nie to czy funkcjonuje jakiś zformalizowany system zarządzania jakością:

……...

Czy Państwa produkty posiadają certyfikaty? TAK / NIE*

Jeśli tak to jakie:

……...

III. Spełnienie wymagań:

Składając formularz (zgodnie z wymaganiami zawartymi w Liście przewodnim) oświadczam, że:

1. Posiadamy uprawnienia do wykonywania określonej działalności lub czynności będących przedmiotem niniejszego zapytania.
2. Posiadamy niezbędną wiedzę i doświadczenie oraz dysponujemy potencjałem technicznym i osobami zdolnymi do wykonywania przedmiotowego zamówienia.
3. Znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

4. Nie jesteśmy w sporze sądowym z KGHM Polska Miedź S.A. lub spółką zależną oraz nie zostało wydane żadne orzeczenie, z którego wynika, że KGHM Polska Miedź S.A. lub spółce zależnej przysługują roszczenia odszkodowawcze w stosunku do Wykonawcy.

5. W stosunku do naszej firmy otwarto/nie otwarto** likwidację/likwidacji** i ogłoszono/nie ogłoszono** upadłość/upadłości** (w przypadku otwarcia likwidacji lub ogłoszenia upadłości Wykonawca zobowiązany jest dołączyć do formularza ofertowego w przypadku otwarcia likwidacji lub ogłoszenia upadłości Wykonawca zobowiązany jest dołączyć do formularza ofertowego oryginał lub kopię postanowienia sądu, w stosunku do Wykonawców, co do których otwarto likwidację bądź których upadłość ogłoszono i którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu).

6. Oferowany przedmiot zamówienia jest wolny od wad prawnych i praw majątkowych osób trzecich.

IV. Załączniki do formularza informacyjnego:

1. Uzupełniony formularz pomocniczy – arkusz oceny

2. Udokumentowane co najmniej 2 wdrożenia w środowiskach o podobnej wielkości oraz specyfiki rodzaju przetwarzanych informacji

3. Referencje / certyfikaty – potwierdzenie kompetencji w zakresie wdrażanego

4. Oferent musi być autoryzowanym partnerem producenta rozwiązania bądź producentem rozwiązania –złożenie oświadczenia

5. Wskazane jest aby rozwiązanie było obecne na liście Gartnera lub musi pochodzić od producenta który jest uznaną marką w zakresie weryfikowanego obszaru technologicznego

6. Gotowość do certyfikacji zgodnie z wymaganiami ustawy o KSC – złożenie oświadczenia

7. W przypadku konieczności przekazania dodatkowych danych związanych ze stosowaną technologią w organizacji przez zamawiającego oferent wyraża zgodę na podpisanie dokumentu o zaufaniu poufności (NDA). – wymagane oświadczenie o wskazanej treści

UWAGA. Niniejsze zapytanie jest procesem dialogu technicznego wraz z badaniem rynku potencjalnych wykonawców, natomiast odesłany wypełniony formularz ma charakter informacyjny.

Podpis i pieczęć osoby uprawnionej do reprezentowania firmy