Kuratorium Oświaty w Łodzi
Al. Tadeusza Kościuszki 120 a
90-446 Łódź
tel.(42) 637-70-55 fax (42) 636-03-85

Znak sprawy: ŁKO.WO.272.274.2022

Łódź, dn. 05.12.2022 r.

Odpowiedzi na pytania

Dotyczy: *: postępowania nr ŁKO.WO.272.274.2022, którego przedmiotem zamówienia jest dostawa sprzętu i oprogramowania komputerowego.*

W związku z wpłynięciem pytań do przedmiotowego postępowania, Zamawiający działając na podstawie art. 284 ust. 1-2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) zwanej dalej „ustawą pzp", udziela następujących odpowiedzi:

Pytanie 1: „Prosimy Zamawiającego o określenie ilości wymaganych licencji."

Odpowiedź: Zamawiający wymaga dostawy 250 licencji. w związku z powyższym działając zgodnie z art. 286 ust. 1 ustawy pzp zmienia treść załącznika nr 2 do SWZ „Formularz oferty" w zakresie części 4 dostawa systemu DLP, gdzie w kolumnie „Liczba" wpisuje wartość 250. Poprawioną wersję edytowalną załącznika nr 2 Zamawiający publikuje wraz z niniejszymi odpowiedziami.

Pytanie 2: „Czy dopuszczany jest system, który umożliwia shadowing kopiowanych danych dla urządzeń zewnętrznych podłączanych do komputera (pendrive, dyski hdd) oraz danych przesyłanych przez przeglądarkę, pocztę e-mail lub synchronizację z chmurami takimi jak OneDrive, Dysk Google?"

Odpowiedź: Dopuszczamy zaoferowanie systemu, który musi umożliwiać shadowing kopiowanych danych dla urządzeń zewnętrznych podłączanych do komputera (pendrive, dyski hdd) jak również schowka systemowego lub alternatywnie dla schowka danych przesyłanych przez przeglądarkę i pocztę e-mail. System musi jednak umożliwiać albo shadowing kopiowanych danych na urządzenia mobilne (iPhone, Windows Mobile, Android) albo zablokowanie podłączenia takich urządzeń do komputera.

Pytanie 3: „Czy dopuszczany jest system, który umożliwia gromadzenie logów audytu centralne w bazie, ale pliki shadowingu są przechowywane lokalnie na końcowych komputerach w formie zaszyfrowanej, uniemożliwiając w ten sposób wyciek danych istotnych dla firmy?."

Odpowiedź: System musi umożliwiać gromadzenie centralnie w bazie danych lub lokalnie logów audytu oraz plików shadowingu (pliki shadowingu przechowywane w bazie lub w zdefiniowanym folderze/udziale sieciowym). Dopuszczamy jednak alternatywnie zaoferowanie systemu, który umożliwia gromadzenie logów audytu centralne w bazie, ale pliki shadowingu przechowuje lokalnie na końcowych komputerach w formie zaszyfrowanej, uniemożliwiając w ten sposób wyciek danych istotnych dla firmy.

Pytanie 4: „Czy dopuszczany jest system, który celem bezpieczeństwa przechowuje pliki shadowingu w formie zaszyfrowanej, niescentralizowanej oraz przechowujący logi audytu w bazie danych oraz retencja i rezerwacja miejsca możliwa jest przez skrypty udostępniane przez producenta?"

Odpowiedź: System musi umożliwiać definiowanie miejsca oraz sposobu lokalnego przechowywania logów audytu i plików shadowingu (rezerwacja miejsca na dysku na pliki

Kuratorium Oświaty w Łodzi
Al. Tadeusza Kościuszki 120 a
90-446 Łódź
tel.(42) 637-70-55 fax (42) 636-03-85

shadowingu, określenie retencji logów audytu i plików shadowingu). Dopuszczamy jednak alternatywnie zaoferowanie systemu, który celem bezpieczeństwa przechowuje pliki shadowingu w formie zaszyfrowanej, niescentralizowanej, a logi audytu przechowuje w bazie danych pozwalając określić retencję i rezerwację miejsca przy użyciu skryptów udostępnionych przez producenta.

Pytanie 5: „Czy dopuszczany jest system, który umożliwia dopisania do alertu linku do polityki bezpieczeństwa, adres e-mail inspektora danych osobowych, logo firmy oraz posiada wbudowane alerty w zależności od naruszenia polityki?"

Odpowiedź: System musi umożliwiać definiowanie treści komunikatów powiadomień wyświetlanych w razie wykrycia incydentu bezpieczeństwa w określonym kontekście działania użytkownika wraz z możliwością dopisania dodatkowych informacji np.: link do polityki bezpieczeństwa oraz dane Inspektora Ochrony Danych Osobowych. Dopuszczamy jednak alternatywnie zaoferowanie systemu który posiada wbudowane alerty w zależności od naruszenia polityki ale pozwala na dopisanie do alertu linku do polityki bezpieczeństwa, adresu e-mail inspektora danych osobowych oraz loga firmy.

Pytanie 6: „Czy dopuszczany jest system, który umożliwia kontrolę dostępu na poziomie użytkownika lub grupy użytkowników do dowolnego typu drukarek włącznie z drukarkami lokalnymi, sieciowymi i wirtualnymi, portów USB i Fire Wire, COM, LPT, Bluetooth, IrDA, czytniki kart oraz w przypadku bluetooth system umożliwia podłączanie urządzeń po bluetooth - ale z rozgraniczeniem na możliwość przesyłania plików na podłączony nośnik, tak, aby dalej można było podłączać słuchawki lub inne urządzenia HiD i z nich korzystać po w/w protokole?"

Odpowiedź: System musi umożliwiać kontrolę dostępu na poziomie użytkownika lub grupy użytkowników do dowolnego typu drukarek włącznie z drukarkami lokalnymi, drukarkami sieciowymi i wirtualnymi, portów USB i Fire Wire, IrDA, COM, LPT, oraz Bluetooth, dopuszczamy jednak alternatywnie kontrolę urządzeń WiFi, urządzeń PDA i smartfonów wykorzystujących system Windows Mobile, Android i iPhoneOs, urządzeń zewnętrznych podłączanych do komputera umożliwiających zapis/odczyt chronionych danych, urządzeń pracujących pod kontrolą protokołu MTP, napędów optycznych CD/DVD/BR, napędów taśmowych, schowka systemowego (z możliwością określenia typu kopiowanych danych: teks, pliki graficzne, pliki audio, zrzut ekranu), mapowanych dysków dla sesji terminalowych, urządzeń USB, portów COM dla sesji terminalowych, schowka systemowego na poziomie sesji terminalowych, dysków HDD, napędów optycznych CD/DVD/BR, schowka systemowego (z możliwością określenia typu kopiowanych danych: teks, pliki graficzne, pliki audio, zrzut ekranu), mapowanych dysków dla sesji terminalowych, urządzeń USB, portów COM dla sesji terminalowych, schowka systemowego na poziomie sesji terminalowych, dysków HDD.

Pytanie 7: „Czy dopuszczany jest system, który umożliwia określenie elementów zachowania użytkownika, które mają być kontrolowane na podstawie kategorii: aplikacje, urządzenia, strony internetowe, drukowanie, ruch sieciowy, wiadomości e-mail, pliki?"

Odpowiedź: System musi umożliwiać określenie rodzajów urządzeń, które mają być kontrolowane (HID, drukarka, skaner, itp.). Dopuszczamy jednak alternatywnie system, który umożliwia określenie elementów zachowania użytkownika, które mają być kontrolowane na podstawie kategorii ale oprogramowanie musi wyróżniać co najmniej następujące kategorie: aplikacje, urządzenia, strony internetowe, drukowanie, ruch sieciowy, wiadomości e-mail i pliki .

Kuratorium Oświaty w Łodzi
Al. Tadeusza Kościuszki 120 a
90-446 Łódź
tel.(42) 637-70-55 fax (42) 636-03-85

Pytanie 8: „Czy dopuszczany jest system działający również na serwerach terminalowych lub/i na maszynach wirtualnych?"

Odpowiedź: System musi umożliwiać wsparcie dla sesji terminalowych (Microsoft, Citrix, VMware) ale dopuszczamy zaoferowanie systemu działającego również na serwerach terminalowych lub/i na maszynach wirtualnych.

Pytanie 9: „Czy dopuszczany jest system, który umożliwia rozpoznawanie plików po zawartości, przez co system je kategoryzuje i stosuje przypisane przez użytkownika reguły?"

Odpowiedź: System musi umożliwiać rozpoznawanie plików po nagłówkach lub po zawartości, przez którą system je kategoryzuje i umożliwiać przypisanie określonych reguł bezpieczeństwa.

Pytanie 10: „Czy dopuszczany jest system, który umożliwia zdefiniowanie ile wystąpień danych słów kluczowych musi wystąpić, aby podjęte zostały działania?"

Odpowiedź: System musi umożliwiać przypisanie wagi do poszczególnych słów oraz progu odcięcia (wartość graniczna, od której podjęte zostaną określone działania). Dopuszczamy jednak zaoferowanie systemu, który umożliwia zdefiniowanie ile wystąpień danych słów kluczowych musi wystąpić, aby podjęte zostały działania.

Pytanie 11: „Czy dopuszczany jest system, który umożliwia wykrywanie oparte na typie plików (rozszerzeniu) lub zawartości pliku?"

Odpowiedź: Dopuszczamy zaoferowanie systemu, który musi umożliwiać wykrywanie oparte na typie plików (rozpoznawanie typu pliku po jego nagłówku lub po ego rozszerzeniu) lub zawartości pliku.

Pytanie 12: „Czy dopuszczany jest system umożliwiający wykrywanie oparte na typie plików - dowolnego rozszerzenia zdefiniowanego przed administratora?"

Odpowiedź: Dopuszczamy zaoferowanie systemu, który musi umożliwiać wykrywanie oparte na właściwościach plików (nazwa, rozmiar, ochrona hasłem, data/czas utworzenia/modyfikacji, rozmiar, szczegóły: autor, nagłówek itp.) lub typie pliku (dla dowolnego rozszerzenia zdefiniowanego przez administratora).

Pytanie 13: „Czy dopuszczany jest system, który umożliwia konfigurację słów kluczowych do wykrywanie wraz z użyciem Regex, czego celem może być wykrywanie różnych form danego słowa?"

Odpowiedź: System musi posiadać wbudowaną analizę fleksyjną dla języka polskiego lub umożliwiać konfigurację słów kluczowych do wykrywanie wraz z użyciem Regex, czego celem może być wykrywanie różnych form danego słowa.

Pytanie 14: „Czy dopuszczany jest system, który umożliwia analizę treści plików skompresowanych w zakresie formatów: .7z, .ace, .arj, .bz, .bz2, .bzip, .bzip2, .car, .gz, .gzi, .gzip, .ice, .rar, .sfx, .tar.gz, .taz, .zip?"

Odpowiedź: Dopuszczamy zmianę zapisu na: System musi umożliwiać analizowanie treści plików skompresowanych co najmniej w zakresie formatów 7z, ZIP, GZIP, BZIP2, TAR, RAR, ARJ.

Pytanie 15: „Czy dopuszczany jest system, który umożliwia określenie harmonogramu skanowania w cyklu dziennym, tygodniowym lub miesięcznym wraz z możliwością wybrania jaki komputer ma

Kuratorium Oświaty w Łodzi
Al. Tadeusza Kościuszki 120 a
90-446 Łódź
tel.(42) 637-70-55 fax (42) 636-03-85

skanowań daną lokalizację (w przypadku lokalizacji sieciowych) oraz wybrania za pomocą jakiego użytkownika ma odbywać się takie skanowanie?"

Odpowiedź: System musi umożliwiać określenia harmonogramu skanowania (skanowanie powtarzane co n godzin, skanowanie powtarzane przez n dni, skanowanie w cyklu tygodniowym lub miesięcznym) oraz określenie priorytetu dla usługi skanowania i maksymalnego czasu skanowania zasobów. Dopuszczamy jednak alternatywnie system, który umożliwia określenie harmonogramu skanowania w cyklu dziennym, tygodniowym lub miesięcznym wraz z możliwością wybrania jaki komputer ma skanować daną lokalizację (w przypadku lokalizacji sieciowych) oraz wybrania za pomocą jakiego użytkownika ma odbywać się takie skanowanie.

Pytanie 16: „Czy dopuszczany jest system, który umożliwia kontrolę ruchu sieciowego na poziomie użytkownika lub grupy użytkowników oraz aplikacji/usług sieciowych dla protokołów: FTP/FTPS, HTTP/HTTPS, SMB, SMTP, MAPI, POP3."

Odpowiedź: Dopuszczamy zmianę zapisu na: System musi umożliwiać kontrolę ruchu sieciowego na poziomie użytkownika lub grupy użytkowników oraz aplikacji/usług sieciowych dla protokołów: FTP/FTPS, HTTP/HTTPS, SMB, SMTP, MAPI.

Pytanie 17: „Czy dopuszczany jest system, który zezwala na kontrolę ruchu sieciowego na poziomie użytkownika systemu operacyjnego komputera dla udostępnianych plików w chmurze, zarówno dla aplikacji Box Sync, Dropbox, Google Drive, OneDrive, Sharepoint jak i dla wersji przeglądarkowych?"

Odpowiedź: Dopuszczamy zmianę zapisu na: System musi umożliwiać kontrolę ruchu sieciowego na poziomie użytkownika system operacyjnego komputera dla udostępnianych plików w chmurze co najmniej dla Dropbox, Google Drive i OneDrive/SkyDrive.

Pytanie 18: „ (...) części nr 4 - dostawa systemu DLP: Na jaką liczbę licencji ma zostać złożona oferta ?"

Odpowiedź: Tak jak w odpowiedzi na pytanie nr 1 zamawiający wymaga 250 licencji.

W związku z udzielonymi odpowiedziami Zamawiający przypomina, że termin składania ofert upływa w dniu **08.12.2022** do godz.**13:00**, otwarcie ofert nastąpi w dniu **08.12.2022** r. o godz. **13:30.**

Z up. Łódzkiego Kuratora Oświaty
Andrzej [illegible]
Łódzki Wicekurator Oświaty