Ministerstwo Rozwoju i Technologii **Warszawa, 09.11.2022 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na dostawę nieograniczonych w czasie licencji oprogramowania audytującego dla 1200 użytkowników wraz z 36 miesięcznym okresem wsparcia technicznego.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego na dostawę 1200 sztuk nieograniczonych w czasie licencji oprogramowania audytującego wraz z 36 miesięcznym okresem wsparcia technicznego.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest dostawa nieograniczonych w czasie licencji oprogramowania audytującego dla 1200 użytkowników wraz z 36 miesięcznym okresem wsparcia technicznego.

II. TERMIN REALIZACJI ZAMÓWIENIA

W terminie **do …… dni** (do uzupełnienia przez Wykonawcę w formularzu ofertowym) od daty podpisania przez strony umowy Wykonawca dostarczy Zamawiającemu nieograniczonych w czasie licencji oprogramowania audytującego dla 1200 użytkowników wraz z 36 miesięcznym okresem wsparcia technicznego wraz z dokumentem potwierdzającym nabycie przez ministerstwo praw do dostarczonego oprogramowania wraz z 36 miesięcznym wsparciem technicznym.

III. MINIMALNE WYMAGANIA DOTYCZĄCE OPROGRAMOWANIA AUDYTUJĄCEGO STANWOIĄCEGO PRZEDMIOT ZAMÓWIENIA

1. Dostarczone oprogramowanie audytujące musi zawierać narzędzia audytujące dla:
   1) poczty Exchange,
   2) Active Directory, Azure AD oraz Office365,
   3) bazy danych SQL Server,
   4) File Server oraz Security Explorer,
   5) Vmware,
   6) SharePoint i OneDrive for Business.
2. Gromadzić i przechowywać zdarzenia w bazie MS SQL.
3. Zapisane zdarzenia audytowe ze wszystkich systemów udostępniać z jednego interfejsu dla audytora/administratora/oficera bezpieczeństwa.
4. Dostarczać raporty o zdarzeniach w sposób ujednolicony (jednolite raporty ze wszystkich audytowanych systemów).
5. Dostarczać mechanizmy delegowania dostępów do produktu (za pomocą ról; RBAC).
6. Oprogramowanie powinno dostarczać informacje o zmianie takie jak: wartości zmiany przed i po zmianie, IP komputera/nazwa komputera, z której została wykonana zmiana, nazwa komputera, na którym zmiana została wykonana, konto użytkownika, z którego została dokonana zmiana, czas wykonania zmiany.
7. Umożliwiać opisywanie zdarzeń.
8. Umożliwiać wykluczenie procesu z audytu (np. agent oprogramowania AV lub agent systemu backupu).
9. Umożliwiać rejestrację zmian nawet w przypadku braku połączenia z serwerem zarządzającym audytem.
10. Umożliwiać generowanie kompleksowych raportów wg. najlepszych praktyk i regulacji m.in. standardów zgodności dla SOX, PCI-DSS, HIPAA, FISMA, GLBA
11. Przekształcać informacje w inteligentne, szczegółowe analizy danych.
12. Przekształcać informacje w inteligentne alarmy.
13. Umożliwiać instalację agenta z konsoli administratora.
14. Rejestrować w logu wszystkie audytowane zdarzenia pokazując jednocześnie wartości przed i po zmianie, IP komputera oraz konto użytkownika, z którego akcja została wykonana.

15. Umożliwiać szybkie tworzenie własnych raportów oraz ich dopasowanie do potrzeb odbiorcy.
16. Umożliwiać w prosty sposób export i/lub import całej i/lub częściowej konfiguracji audytowanych zasobów oraz konfiguracji narzędzia (grupy, użytkownicy, uprawnienia etc).
17. Bazować na niezależnym/własnym audycie monitorowanych systemów Microsoft – tworzenie własnego audytu za pomocą agenta instalowanego na monitorowanym systemie.

A. <u>Minimalne wymagania w zakresie narzędzia audytujące do poczty Exchange:</u>

Narzędzie audytujące do poczty Exchange musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać audyt bezpieczeństwa serwera pocztowego MS Exchange 2019.
2. Umożliwiać monitorowanie dostępu do skrzynki osób nie będących jej właścicielami, w szczególności aktywność takiej osoby na obiektach poczty.
3. Umożliwiać monitorowanie dostępu właściciela do swojej skrzynki.
4. Umożliwiać rejestrowanie zmian w uprawnieniach klienckich oraz w delegowaniu uprawnień do skrzynki.
5. Umożliwiać rejestrowanie zmian w uprawnieniach do skrzynek.
6. Umożliwiać rejestrowanie zmian w atrybutach AD związanych z serwerem Exchange,
7. Generować w dzienniku zdarzeń Microsoft szczegółowe logi aktywności użytkowników oraz zmian w środowisku Exchange.
8. Umożliwiać blokowanie określonych skrzynek pocztowych Exchange przed jakimikolwiek modyfikacjami nawet jeśli administrator ma do tego przyznane uprawnienia natywne Windows.
9. Umożliwiać zablokowanie zmian z określonej lokalizacji sieciowej.
10. Prezentować statystyki zmian i aktywności online (najlepiej w formie wykresów kołowych) na serwerach Exchange.
11. Dostarczać informacje o zmianie uprawnień do skrzynki takie jak: wartości zmiany atrybutu przed i po zmianie, IP komputera/nazwa komputera, z której została wykonana zmiana, nazwa komputera, na którym zmiana została wykonana, konto użytkownika, z którego została dokonana zmiana, czas wykonania zmiany,
12. Umożliwiać w prosty sposób wykluczanie kont użytkowników lub skrzynek pocztowych, których nie chcemy objąć audytem,
13. Umożliwiać opisywanie zdarzeń administracyjnych wykonanych w środowisku Exchange na skrzynkach pocztowych.
14. Rejestrować zdarzenia zmian w konfiguracji usług, rejestru systemowego oraz lokalnych użytkowników/grup użytkowników na serwerze Exchange.
15. Zapewniać pobieranie informacji o użytkowniku oraz grupach Active Directory do których należy.
16. Umożliwiać opisywanie zdarzeń.
17. Zagwarantować zarządzanie oraz monitorowanie agentów z jednego centralnego miejsca.
18. Posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób za pomocą e-mail.
19. Zapewniać raportowanie oraz budowanie własnych raportów bezpośrednio z konsoli oraz ich eksport i zapis do różnych formatów np. PDF, HTML, CSV, XLS, RTF, TXT.
20. Umożliwiać przegląd raportów z poziomu przeglądarki internetowej.
21. Umożliwiać szybkie tworzenie własnych raportów oraz ich dopasowanie.
22. Umożliwiać Śledzenie aktywności „non-owner”:
    1) Logowanie do skrzynki innego użytkownika,
    2) Logowanie do skrzynki innego użytkownika przez OWA,
    3) Otwarcie folderu w skrzynce pocztowej,
    4) Dostęp do elementów poczty (kalendarz, notatki, kontakty),
    5) Odczyt, modyfikacja, przekierowanie, kasowanie wiadomości w skrzynce użytkownika,
    6) Śledzenie aktywności “send-as” (zmiany w atrybutach AD oraz w konfiguracji Exchange).
23. Monitorowanie tworzenia/kasowania skrzynek.
24. Audytowanie tematów wiadomości.
25. Śledzenie dostępu właściciela do swojej skrzynki.
26. Rejestrowanie zmian w uprawnieniach klienckich oraz w delegowaniu uprawnień.
27. Rejestrowanie zmian w konfiguracji protokołów Exchange.
28. Rejestrowanie zmian w uprawnieniach do skrzynek.

29. Umożliwiać tworzenie raportów online oraz historycznych na temat zmian konfiguracyjnych w środowisku Active Directory/Windows/Exchange.

B. <u>Minimalne wymagania w zakresie narzędzia audytujące do Active Directory/Azure AD</u>

Narzędzie audytujące do Active Directory/Azure AD musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać rejestrację zmiany w schemacie Active Directory oraz w konfiguracji kontrolerów domeny.
2. Prezentować statystyki zmian online (najlepiej w formie wykresów kołowych) w domenie ActiveDirectory/Windows.
3. Umożliwiać prezentację na bieżąco zmian w Active Directory/Windows.
4. Udostępniać szczegółowe informacje dotyczące zmian i prób zmian, takich jak nieuprawnione akcje administracyjne na obiektach GPO/AD.
5. Umożliwiać rejestrację zmian w konfiguracji usług, rejestru systemowego.
6. Umożliwiać selekcję atrybutów obiektów Active Directory do audytu.
7. Monitorować krytyczne logi bezpieczeństwa.
8. Umożliwiać definiowanie własnych użytkowników i grup bezpieczeństwa mających dostęp do narzędzia (definiowane role użytkowników).
9. Instalacja, zarządzanie oraz monitorowanie agentów powinna odbywać się z centralnego miejsca.
10. Umożliwiać definiowanie lub korzystanie z wbudowanych logicznych kolekcji komputerów, na których będą zbierane i monitorowane logi.
11. Posiadać funkcjonalność zabezpieczania krytycznych obiektów w katalogu AD oraz obiektach GPO przed modyfikacją, zmianą, kasowaniem i tworzeniem.
12. Umożliwiać zablokowanie zmian z określonej lokalizacji sieciowej.
13. Umożliwiać filtrowanie raportów po dowolnych polach i atrybutach (zakres czasu, użytkownicy, komputery, typ zdarzeń, itp.).
14. Umożliwiać tworzenie raportów graficznych.
15. Zabezpieczać logi przed ich utratą po stronie systemu operacyjnego w szczególności w sytuacjach takich jak wyczyszczenie logów bądź nadpisanie.
16. Zapewniać łatwą instalację agentów poprzez sieć.
17. Umożliwiać wyszukiwanie zdarzeń użytkownika bądź obiektu.
18. Umożliwiać przeprowadzanie inspekcji zmian na katalogu AD w wersji 2012 R2/2016/2019 bez włączania natywnego audytu Microsoft.
19. Rejestrować zdarzenia zmian w konfiguracji usług, rejestru systemowego oraz lokalnych grup użytkowników na kontrolerach domeny.

C. <u>Minimalne wymagania w zakresie narzędzia audytujące do bazy danych SQL Server</u>

Narzędzie audytujące do bazy danych SQL Server musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać inspekcję bazy danych w celu zabezpieczenia danych bazy SQL.
2. Zawierać rozbudowany i konfigurowalny audyt,
3. Umożliwiać raportowanie dla krytycznych zmian w SQL w tym:
    1) Brokera,
    2) silnika bazy danych,
    3) obiektów,
    4) zdarzeń transakcji,
    5) błędy i ostrzeżenia,
    6) zmiany danych.
4. Umożliwiać audyt zmian w konfiguracji bazy/instancji SQL.

5. Umożliwiać kontrolować zasady przez śledzenie aktywności użytkowników i administratorów.
6. Umożliwiać audyt dodawania i usuwania baz danych.
7. Umożliwiać audyt zmiany uprawnień do baz SQL.
8. Umożliwiać audyt zmiany konfiguracji baz i instancji MS SQL.
9. Umożliwiać audyt zmian w rejestrze systemowym serwera MS SQL.
10. Umożliwiać audyt zmian usług systemu Windows,
11. Umożliwiać szczegółowy audyt bazy (np. dodanie/usunięcie indeksu, dodanie/usunięcie „foregin key" etc.).
12. Umożliwiać audyt „Data Layer" umożliwiający dostarczenie informacji ktdokonał zmian w tabeli np. Insert Row, Delete Row, Update Row etc.

D. <u>Minimalne wymagania w zakresie narzędzia audytujące do File Server oraz Security Explorer</u>

Narzędzie audytujące do File Server oraz Security Explorer musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać przeprowadzanie inspekcji zmian na folderach, udziałach sieciowych oraz plikach znajdujących się na systemach Windows 2012 R2/2016/2019 bez włączania natywnego audytu Microsoft.
2. Wspierać system plików FAT32 oraz NTFS.
3. Generować w dzienniku zdarzeń Microsoft szczegółowe logi aktywności użytkowników oraz zmian na plikach i folderach.
4. Prezentować statystyki zmian i aktywności online (najlepiej w formie wykresów kołowych) na serwerach plików.
5. Umożliwiać zablokowanie zmian z określonej lokalizacji sieciowej.
6. Na bieżąco pokazywać zmiany na zasobach Serwerów Plików Windows.
7. Dostarczać informacje o zmianie na pliku (nazwa, właściciel oraz uprawnienia) takie jak: wartości zmiany atrybutu przed i po zmianie, IP komputera/nazwa komputera, z której została wykonana zmiana, nazwa komputera, na którym zmiana została wykonana, konto użytkownika, z którego została dokonana zmiana, czas wykonania zmiany.
8. Umożliwiać rejestrację zmian w konfiguracji usług, rejestru systemowego oraz lokalnych użytkowników/grup użytkowników na serwerach Windows.
9. Umożliwiać w prosty sposób zapis, import i eksport ustawień audytu na folderach/plikach oraz udziałach sieciowych.
10. Umożliwiać w prosty sposób wykluczanie procesów (aplikacji) lub kont użytkowników, których nie chcemy objąć audytem.
11. Umożliwiać blokowanie określonego folderu/udziału sieciowego przed niechcianą aktywnością użytkownika.
12. Umożliwiać rejestrację w logu informacji dotyczących odczytu, zapisu, przenoszenia, kasowania, zmiany nazwy, utworzenia, zmiany właściciela, zmiany uprawnień do pliku lub folderu na serwerze Windows pokazując jednocześnie wartości zmiany przed i po zmianie, IP komputera oraz konto użytkownika, z którego została dokonana zmiana/dostęp do pliku/folderu.
13. Pokazywać w logu zmian pełną ścieżkę do pliku, bądź katalogu.
14. Umożliwiać zarządzanie uprawnieniami na poziomie:
    1) NTFS,
    2) Zasobów udostępnionych,
    3) Rejestru,
    4) Drukarek,
    5) Usług,

6) Harmonogramu zadań,
7) Grup i użytkowników,
8) SharePoint,
9) SQL Server

15. Umożliwiać określenie, kto ma prawa do zasobów w całej organizacji i z czego one wynikają (inherited) permission, direct assigment, nested groups).
16. Umożliwiać nadawanie, odwoływanie, klonowanie, modyfikowanie i nadpisywanie uprawnień z centralnej lokalizacji.
17. Umożliwiać tworzenia kopii zapasowych i przywracania tylko uprawnień, zapewniając integralność danych.
18. Posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób za pomocą e-mail.
19. Zapewniać raportowanie oraz budowanie własnych raportów bezpośrednio z konsoli oraz ich eksport i zapis do różnych formatów np. PDF, HTML, CSV, XLS, RTF, TXT
20. Umożliwiać opcje odwoływania uprawnień - usuwanie uprawnień dla nieznanych i usuniętych kont.
21. Umożliwiać identyfikację i czyszczenie uprawnień po migracji i/lub na istniejących zasobach.

E. <u>Minimalne wymagania w zakresie narzędzia audytujące do Vmware</u>

Narzędzie audytujące do Vmware musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać szczegółowy audyt instancji zdarzeń dla infrastruktury VMware vCenter.
2. Umożliwiać audyt zdarzeń zmian konfiguracji maszyn wirtualnych.
3. Umożliwiać audyt konfiguracji przed i po wykonaniu zmian.
4. Umożliwiać audyt zdarzeń dla obiektów:
   1) Użytkowników,
   2) Serwerów ESX,
   3) Folderów,
   4) Klastrów,
   5) Puli zasobów,
   6) Maszyn wirtualnych.
5. Umożliwiać tworzenie raportów w różnych formatach np. PDF, HTML, CSV, XLS, RTF, TXT.
6. Posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób w odpowiednim formacie.
7. Umożliwiać przegląd raportów z poziomu przeglądarki internetowej.
8. Umożliwiać rejestrację zmian nawet w przypadku braku połączenia z serwerem zarządzającym audytem.

F. <u>Minimalne wymagania w zakresie narzędzia audytujące do SharePoint i OneDrive for Business</u>

Narzędzie audytujące do SharePoint i OneDrive for Business musi spełniać minimum poniżej opisane wymagania:

1. Umożliwiać audyt bezpieczeństwa zasobów MS SharePoint Online.
2. Umożliwiać audyt zmian uprawnień na zasobach farmy MS SharePoint Online.
3. Umożliwiać audyt zmian dla zasobów OneDrive for Business.
4. Umożliwiać rejestrację zmian w konfiguracji audytu,
5. Umożliwiać audyt zmian w konfiguracji witryn (np. włączenie wersjonowania).
6. Umożliwiać rejestrację zdarzeń związanych ze zmianą uprawnień do zasobów SharePoint takich jak kolekcja witryn, witryna, dokument.
7. Umożliwiać tworzenie raportów online oraz historycznych na temat zmian konfiguracyjnych w środowisku Active Directory/Windows/MS SharePoint Online.

8. Umożliwiać tworzenie raportów w różnych formatach, minimum w: PDF, HTML, CSV, XLS, RTF, TXT.
9. Posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób w odpowiednim formacie,
10. Umożliwiać przegląd raportów z poziomu przeglądarki internetowej.
11. Umożliwiać rejestrację zmian nawet w przypadku braku połączenia z serwerem zarządzającym audytem.

G. <u>Minimalne wymagania w zakresie wsparcia technicznego do dostarczonego oprogramowania audytującego</u>

Wykonawca do dostarczonego oprogramowania zapewni wsparcie techniczne na okres 36 miesięcy od daty instalacji. Wykonawca dostarczy dokument potwierdzający nabycie przez ministerstwo praw do dostarczonego oprogramowania wraz z 36 miesięcznym wsparciem technicznym.

W ramach wsparcia technicznego Zamawiający będzie miał prawo do:

1. aktualizacji oprogramowania do najnowszych wersji, aktualizacji i poprawek dostępnych w okresie obowiązywania umowy oraz ich instalację;
2. nieograniczonej liczby zgłoszeń błędów, awarii, nieprawidłowego działania oprogramowania pięć dni w tygodniu w godzinach 8:00-16:00 za pomocą strony www lub dedykowanego w tym celu numeru telefonu;
3. dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania;
4. dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, założenie zgłoszenia awarii u producenta, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania.