**Załącznik nr 1 do OPZ**

**Znak sprawy: PK XII BIA 0470.11.2020**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Specyfikacja techniczna**

**Liczba licencji (obsługa 3 domen) ……………………….**

**Producent ………………………………………………………………………\***

**Nazwa i wersja oprogramowania ………………………………………………………………………\***

Zamawiający zastrzega sobie prawo wezwania oferenta do dostarczenia ogólnie dostępnej dokumentacji oferowanego oprogramowania potwierdzającej spełnienie wybranych wymaganych/oferowanych funkcjonalności (może być wymagane wskazanie odpowiednich fragmentów dokumentacji). Niedostarczenie wymaganej ogólnodostępnej dokumentacji, będzie równoznaczne z odrzuceniem oferty.

**Wymagania funkcjonalne** **systemu audytowania zmian i powiadamiania w rozproszonych środowiskach Active Directory**

1. **Przedmiot i zakres zamówienia**

Przedmiotem zamówienia jest dostawa, wdrożenie i wsparcie techniczne dla oprogramowania służącego do audytowania zmian i powiadamiania w rozproszonych środowiskach Active Directory, zarówno w czasie rzeczywistym jak i wskazanym. W szczególności przedmiot zamówienia zawiera:

* 1. Dostarczenie licencji wieczystej i instalację oprogramowania wraz ze wsparciem technicznym świadczonym w języku polskim przez podmiot do tego upoważniony przez producenta oprogramowania na terenie Polski,
  2. Licencję wieczystą dla 30 kontrolerów pracujących w 3 różnych domenach Active Directory pochodzącą z oficjalnego, polskiego kanału dystrybucji ze wsparciem technicznym na okres 36 miesięcy.
  3. Przeprowadzenie szkoleń z zakresu instalacji, konfiguracji, administracji, obsługi i utrzymania dostarczonego oprogramowania w ilości 24 godzin dla 4 osób.
  4. Instalacja, konfiguracja oprogramowania i uruchomienie produkcyjne zgodnie z przyjętymi procesami procedurami biznesowymi.
  5. Opracowanie projektu technicznego, dokumentacji powdrożeniowej oraz dokumentacji administratora zawierającej w szczególności procedury eksploatacyjne i utrzymaniowe.

1. **Wymagania podstawowe oprogramowania**
2. Dopuszczalny język konsoli użytkownika oprogramowania to język angielski lub język polski
3. System umożliwia audyt zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych
4. System działa bezagentowo
5. System wspiera konfigurację z zewnętrzną bazą danych MSSQL
6. System umożliwia zbiorcze audytowanie środowiska Active Directory, a w szczególności:
   * 1. Nieudane próby zalogowania do środowiska domenowego
     2. Stacje robocze
     3. Serwery
     4. Kontrolery domen
     5. Poprawne logowanie użytkowników wraz z pełną historią logowania
7. Nieudane próby logowania na serwery Radius oraz historię logowań.
8. Zmiany dokonywane na kontach użytkowników, a w szczególności:
   1. Tworzenie kont
   2. Usuwanie kont
   3. Dezaktywacja kont
   4. Modyfikacja haseł
   5. Spis zablokowanych użytkowników
   6. Historie użytkowników
9. Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup.
10. Zmiany dokonane na obiektach komputerów, a w szczególności:
11. Tworzenie kont
12. Usuwanie kont
13. Dezaktywacja kont
14. Historię kont
15. Audut zmian w jednostkach organizacyjnych, a w szczególności:
16. Tworzenie OU
17. Usuwanie OU
18. Lista modyfikowanych OU
19. Historie OU
20. Audyt zmian w zasadach grupowych, a w szczególności:
21. Tworzenie
22. Usuwanie GPO
23. Lista modyfikowanych GPO
24. Historia GPO
25. Zaawansowane zmiany w GPO
26. Audyt zmian uprawnień, a w szczególności:
27. Uprawnienia dotyczące poziomu dostępu do domeny
28. Uprawnienia zmian OU
29. Uprawnienia zmian w kontenerach
30. Uprawnienia zmian w GPO
31. Uprawnienia zmian użytkowników
32. Uprawnienia zmian grup
33. Uprawnienia zmian komputerów
34. Uprawnienia zmian DNS
35. Audyt zmian na serwerach plików, a w szczególności
36. Windows
37. Windows file Cluster
38. EMC
39. Możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania.
    1. Audyt wydruków
    2. Raporty zgodności dla audytów, a w szczególności: SOX,HIPAA,PCI-DSS,GLBA,FISMA, RODO/GDPR
40. Audyt zmian na serwerach członkowskich
41. Audyt stacji roboczych
42. System powinien posiadać moduł powiadomień w formie alertów
43. Widocznych w systemie
44. Drogą mailową
45. Poprzez SMS
46. System umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.
47. System posiada alerty o przekroczonej przestrzeni dyskowej
48. Narzędzie umożliwia zwolnienie zajętej przestrzeni dyskowej
49. System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum.
50. System umożliwia audyt urządzeń USB dla Serwerów Windows 2016 i systemu Windows 10, a w szczególności:
51. Zmiany na plikach lub folderach
52. Odczyt danego pliku
53. Zmiana danego pliku
54. Kopiowane danego pliku
55. System umożliwia analitykę zachowań, pokazując dane sumarycznie , a w szczególności:
    1. Nietypową aktywność danego użytkownika
    2. Nietypową aktywność użytkownika na serwerze
    3. Nietypową ilość prób np. logowań
    4. Nietypowe godziny logowań użytkowników
    5. Nietypowe przydzielenie zasobów (quota) dla danego użytkownika
    6. Nietypowe działania na plikach
56. System obsługuje audytowanie zmian na share’ach sieciowych, w tym:
57. Zmiany nazw plików oraz folderów
58. Utworzenie nowych plików oraz folderów
59. Usunięcie plików oraz folderów
60. Przeniesienie plików oraz folderów
61. Zmiany uprawnień na plikach i folderach
62. System umożliwia przesyłanie logów do SYSLOG’a lub innych systemów SIEM’owych.
63. System obsługuje połączenie LDAP’owe po SSL’u.
64. System pozwala na eksportowanie raportów/danych do formatów: CSV, PDF, XLS, HTML.
65. System dodatkowo obsługuje raportowanie z ADLDS oraz LAPS’a.

**UWAGI ZAMAWIAJĄCEGO:**

(\*) Należy podać nazwę oferowanego sprzętu/oprogramowania, model sprzętu/wersję oprogramowania i producenta.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Czytelny Podpis/podpisy osoby/osób uprawnionego do reprezentowania Wykonawcy**

**Miejscowość\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_\_\_\_**