Załącznik nr 1 do specyfikacji

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie zintegrowanego systemu zarządzania uprzywilejowanymi kontami oraz nagrywania sesji administracyjnych wraz z niezbędnymi licencjami, gwarancją, wsparciem technicznym oraz instruktażem dla administratorów zwanego dalej także „systemem".

I Opis przedmiotu zamówienia:

1. System musi posiadać funkcje zarządzania (automatycznej zmiany haseł, definiowania polityki dostępu) kontami uprzywilejowanymi w:
   a. Systemach operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS 390);
   b. Bazach danych: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, DB2, Informatica, MariaBD, MongoDB, PostgreSQL;
   c. Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, IBM Tivoli RSA authentication Manager, HP iLO, SAP Application Server;
   d. Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Netscreen, F5, Infoblox NIOS, FireEye Malware Analysis, FortiGate, Aruba, PaloAlto Networks, A10, Riverbed, Gemalto;
   e. Aplikacjach typu SaaS/stronach web/interfejsach web, minimum takich jak: Amazon Web Services (klucze AP1 oraz konta uprzywilejowane, konto root), Zarządzanie Microsoft Azure (klucze API oraz konta uprzywilejowane);
   f. Modułach: Microsoft Services, Scheduled tasks, IIS application Pool, IIS Directory Security, w rejestrach, COM+, zarządzanie kontami w domenie Microsoft;
   g. Plikach konfiguracyjnych, tabelach baz danych;
   h. Środowiskach wirtualizacyjnych VMWare ESX/ESXi (vCenter);
2. System musi zapewniać ochronę kont dla dowolnego urządzenia obsługującego ODBC w wersji 2.7 lub wyższej.
3. System musi zapewniać możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania dostępnych nieodpłatnie na oficjalnej stronie producenta rozwiązania. Producent oferowanego systemu powinien udostępniać nie mniej niż 200 unikalnych integracji udostępnionych w ramach wspomnianego portalu.
4. System musi zapewniać możliwość zarządzania kontami uprzywilejowanymi wykorzystywanymi w obrębie systemu docelowego dla systemów spoza listy "out of box" z wykorzystaniem skryptów lub innych mechanizmów realizowanych i wspieranych przez producenta rozwiązania w zakresie zmiany haseł poprzez: SSH / Telnet, API do zewnętrznych aplikacji, możliwość wykonywania zmian oraz weryfikacji spójności haseł poprzez symulację działań użytkownika w sesji aplikacji Web.
5. System musi zapewniać możliwość automatycznego wykrywania kont w nowych urządzeniach Windows, usługach systemu Windows, zaplanowanych zadaniach, kontach serwisowych IIS itp., automatycznego dodania powyższych do systemu oraz automatycznie wymusić odpowiednią politykę zarządzania kontami uprzywilejowanymi.
6. System musi posiadać ochrony/zarządzania oraz dynamicznego generowania (w formie pseudolosowej) nowego klucza SSH zgodne z określonym szablonem.
7. System musi automatycznie porównywać hasło/klucz SSH przechowywane w systemie oraz hasło/klucz SSH przechowywane na systemie docelowym.

8. System musi umożliwiać wykrywanie par kluczy SSH w danej infrastrukturze.
9. System musi umożliwiać zarządzanie i zapewniać bezpieczeństwo kluczy SSH używanych przez aplikacje w przypadku przechowywania kluczy w plikach konfiguracyjnych.
10. System musi automatycznie synchronizować hasło/klucz SSH przechowywane w produkcie oraz hasło/klucz SSH przechowywane na systemie docelowym w przypadku wykrycia niezgodności.
11. System musi umożliwiać przechowywanie historii rotacji haseł (np. trzy ostatnie hasła dla danego systemu docelowego) oraz umożliwiać łatwy dostęp do tej historii (np. poprzez interfejs webowy).
12. System musi umożliwiać zestawienie połączenia oraz monitoring sesji do systemu docelowego bez konieczności uprzedniego przekazania użytkownikowi hasła konta uprzywilejowanego (po uwierzytelnieniu użytkownika oraz wskazaniu konta uprzywilejowanego produkt musi wprowadzić do dowolnie wybranej aplikacji dane dostępowe, dzięki czemu nie muszą być one udostępniane użytkownikowi). System musi udostępniać narzędzia do obsługi aplikacji instalowanych na systemie operacyjnym modułu separacji oraz nagrywania sesji. Jako obsługa rozumiane jest uruchomienie aplikacji oraz wypełnienie pól danymi dostępowymi automatycznie podstawionymi z zabezpieczonego, centralnego repozytorium kont uprzywilejowanych. W przypadku zestawienia połączeń przez przeglądarkę internetową system musi posiadać moduł umożliwiający realizację procesu zmodyfikowania przeglądarki internetowej przez którą realizowana jest sesja uprzywilejowana (np. wyłączanie paska adresu, menu, narzędzi, widok theatermod, blokowanie wpisywania znaków podczas wypełniania danych dostępowych etc.).
13. System musi umożliwiać zestawianie i zarządzanie sesjami uprzywilejowanymi do systemów chronionych:
    a. Systemach operacyjnych: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS 390):
    b. Bazach danych: Microsoft SQL, Oracle, MySQL, SAP HANA, DB2;
    c. Systemach zarządzania infrastrukturą, aplikacjach: DELL DRAC, RSA authentication Manager, HP iLO, SAP GUI, BMCRemedy;
    d. Urządzeniach sieciowych oraz systemach bezpieczeństwa: Cisco (routery, seria nexus, firewalle), HP, Checkpoint, Radware, F5, FortiGate, PaloAlto Networks;
    e. Aplikacjach typu SaaS/ stronach web/ interfejach web, minimum takich jak: Amazon Web Seryices (konsola root, IAM, integracja z STS), Zarządzanie Microsoft Azure;
    f. Środowiskach wizualizacyjnych VMWare ESX/ESXi, vCenter.
14. System musi posiadać wsparcie dla monitoringu i separacji sesji oraz realizacji funkcji Single Sign-On dla kont uprzywilejowanych dla innych aplikacji oraz systemów niż wskazane w punkcie 13, poprzez możliwość wykorzystania nie mniej niż: uruchomienia aplikacji ze wskazanym zbiorem parametrów, zastosowania opisowego języka skryptowego, wbudowanego komponentu pozwalającego na obsługę własnych aplikacji web;
15. System musi przechowywać nagrania sesji w zabezpieczonym kryptograficznie repozytorium uniemożliwiającym ich manipulacje. Żaden z użytkowników włącznie z administratorem systemu nie może mieć wpływu na integralność składowanych nagrań (włącznie z brakiem możliwości ich usunięcia w zdefiniowanym okresie składowania danych);

16. System musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie list dopuszczalnych i niedopuszczalnych poleceń wykonywanych poprzez SSH;
17. System musi zapewniać rozliczalność w przypadku jednoczesnego wykorzystania konta współdzielonego przez więcej niż jednego użytkownika;
18. System musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych (wymagane są nie mniej niż następujące mechanizmy indeksowania: keystrokes, odpowiedzi okien systemu operacyjnego, komendy SQL);
19. System musi umożliwiać monitoring, ingerencję oraz zakończenie aktywnej sesji RDP w czasie jej trwania, a także określenie zbioru poleceń i uruchomionych funkcji systemu operacyjnego które spowodują automatyczne zakończenie / wstrzymanie sesji użytkownika;
20. System musi umożliwiać dostęp użytkowników do zasobu docelowego następującymi narzędziami:
    a. Interfejs Web rozwiązania zabezpieczenia kont uprzywilejowanych;
    b. Wykorzystanie różnych klientów RDP używanych na stacji, z której realizowany jest dostęp uprzywilejowany poprzez nie mniej niż: zdefiniowanie parametrów połączenia w ramach pliku konfiguracyjnego klienta RDP oraz możliwość interaktywnego odpytania użytkownika o właściwości systemu chronionego (takie jak adres, aplikacja kliencka, nazwa konta uprzywilejowanego) do którego będzie zestawione połączenie, przy czym wspierana musi być metoda uwierzytelnienia do systemu bazująca na certyfikatach PKI;
    c. Wykorzystanie przeglądarki internetowej obsługującej html5 w celu zapewnienia wsparcia dla użytkowników korzystających z innych systemów operacyjnych niż Windows (brak klienta RDP na stacji użytkownika). W ramach połączenia realizowanego za pomocą tej metody sesja uprzywilejowana (zestawiona w oparciu o dowolną aplikację skonfigurowaną na systemie proxy) musi być tunelowana w html'u i widoczna dla użytkownika jako nowa zakładka w przeglądarce;
    d. Wykorzystanie różnych klientów linii poleceń i protokołu SSH (np. putty), przy czym wspierana musi być metoda uwierzytelnienia do systemu bazująca na kluczach SSH;
    e. Wykorzystanie dowolnej przeglądarki internetowej (minimum Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox) używanej na stacji roboczej z której realizowany jest dostęp uprzywilejowany do aplikacji Web (np. dostęp administracyjny do konsoli Ażure / AWS/ GCP, salesforce). Opcja ta musi bazować na systemie proxy https z możliwością zapewnienia rozliczalności działań użytkownika. Po uwierzytelnieniu użytkownika na warstwie proxy (uwierzytelnienie na poziomie oferowanego rozwiązania z wykorzystaniem konta nieuprzywilejowanego) hasło konta uprzywilejowanego musi zostać automatycznie wstrzyknięte z centralnego repozytorium do sesji zestawianej z aplikacją chronioną. Przekierowanie ruchu musi bazować minimum na następujących mechanizmach:
        i. konfiguracji proxy przeglądarki, z której realizowany jest dostęp uprzywilejowany, w którym przekierowanie ruchu (sesje do aplikacji chronionych) do proxy realizowane jest przez samą przeglądarkę użytkownika (konfiguracja PAC File),
        ii. konfiguracji reverse proxy umożliwiającej połączenie użytkownika na adres skonfigurowany na proxy (np. połączenie na adres facebook.przyklad.com który jest powiązany z chronioną aplikacją facebook.com)".

21. System musi wspierać tryb automatycznego, tymczasowego przypisywania konta użytkownika systemu Windows do grupy lokalnych administratorów po złożeniu stosownego wniosku;
22. System musi wspierać tryb automatycznego generowania krótkoterminowych certyfikatów SSH w chronionych systemach Linux/Unix dla administratorów po złożeniu stosownego wniosku. Wygenerowane krótkoterminowe certyfikaty muszą być podpisane przez uprzednio utworzony klucz CA oraz zawierać klucz publiczny, informację o tożsamości wnioskującego administratora i opcjonalnie dodatkowe restrykcje przypisanego do wnioskującego;
23. System musi posiadać funkcję kategoryzacji nagranych sesji użytkowników pod kątem ryzyka. Ryzyko opisane musi być poprzez konfigurację przez administratora systemu zbioru wykrywanych w trakcie trwania sesji funkcji /poleceń i przypisanej do nich wagi. Ryzyko musi być analizowane również podczas trwania bieżących sesji. Informacje dotyczące poziomu ryzyka sesji muszą być widoczne zarówno w konsoli monitoringu sesji jak i w interfejsie obrazującym ryzyka i incydenty bezpieczeństwa (dashboard). Administrator musi posiadać możliwość określenia w wyniku których akcji wykonanych przez użytkownika sesja powinna być automatycznie zakończona;
24. System musi posiadać wbudowane narzędzia analityczne umożliwiające automatyczne, bezobsługowe (bez konieczności definiowania reguł polityki bezpieczeństwa) wykrywanie podejrzanej aktywności kont uprzywilejowanych na bazie nauczonych automatycznie wzorców działania poszczególnych użytkowników (podejrzany czas pracy, nowy adres 1P, zbyt duża liczba odwołań do repozytorium kont o hasła);
25. System musi umożliwiać pobieranie danych o aktywnościach użytkowników z zewnętrznych systemów SIEM, system musi obsługiwać w tym celu minimum następujące rozwiązania: Arcsight, Qradar, Splunk, LogRhythm, RSA, McAfee oraz zewnętrzne źródła informacji minimum rsyslog (z systemów Unix/Linux), Windows Event Forwarder (z systemów Windows), AWS CloudTrail;
26. System musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń, które powinny być wysłane do systemu SIEM; System musi umożliwiać integrację z SIEM Splunk
27. System musi wspierać transfer plików w trakcie trwania sesji graficznej;
28. System musi posiadać interfejs REST API do automatyzacji procesu zarządzania użytkownikami;
29. Wymagane jest dostarczenie licencji dla sytemu dla 10 użytkowników.

II Wdrożenie:

1. Wykonanie projektu technicznego wdrożenia, który minimalnie będzie zawierał:
   a. Analizę przedwdrożeniową mającą na celu określenie katalogu kont podlegających ochronie;
   b. Parametry techniczne wdrażanego systemu,
   c. Opis planowanych prac koniecznych do wdrożenia systemu wraz z informacjami o niezbędnych wyłączeniach systemów działających oraz długości ich trwania
   d. Wyniki analizy konfiguracji obecnie posiadanego przez Zamawiającego systemu;
   e. Podział na etapy wdrażania systemu: konta systemów operacyjnych, konta baz danych, wykrywanie za pomocą narzędzia wyszukiwania kont.
   f. Harmonogram wdrożenia dostarczonego rozwiązania uwzględniający iż wszelkie

prace powodujące przerwy w działaniu sieci i systemów Zamawiającego można wykonywać tylko i wyłącznie w weekendy po wcześniejszym uzgodnieniu

2. Instalacja systemu w infrastrukturze Zamawiającego:
   a. Instalacja poszczególnych elementów systemu w środowisku Zamawiającego; Jeśli system będzie dostarczony jako appliance to instalacja sprzętu w szafie rack w budynkach na terenie Krakowa; jeśli system będzie dostarczony jako wirtualny to instalacja odpowiednich systemów na wirtualizatorze Zamawiającego (klaster serwerów Hyper-V w wersji 2012R2).
   b. Konfiguracja elementów systemu zgodnie z wykonanym i zatwierdzonym przez Zamawiającego projektem technicznym (m.in. migracja kont uprzywilejowanych do systemu, konfiguracja narzędzi pozwalających na zestawienia połączenia z systemami chronionymi bez przekazywania danych dostępowych na stację użytkownika). Konfiguracja modułu zdalnego dostępu do infrastruktury;
   c. Przeniesienie konfiguracji z aktualnie posiadanego przez Zamawiającego systemu;
   d. Integracja z systemami infrastruktury Zamawiającego:
      i. ActiveDirectory dla użytkowników;
      ii. SIEM Splunk dla monitorowania systemu i przekazywania logów;
      iii. Microsoft Exchange dla wymiany informacji poprzez pocztę elektroniczną,
      iv. System kopii zapasowej
3. Po wykonaniu wdrożenia Wykonawca przygotuje powdrożeniową dokumentację techniczną, zawierającą minimum opis wykonanych prac i konfigurację systemu, a także wykona testy poprawności pracy systemu, funkcjonalne oraz wysokiej dostępności.
4. Przeprowadzenie praktycznego instruktażu dla co najmniej dwóch administratorów systemu w miejscu i terminie uzgodnionym z Zamawiającym trwającego nie mniej niż 40 godzin.

III Wsparcie techniczne i Gwarancja:

1. gwarancja producenta oferowanego systemu min. 36 miesięcy od daty podpisania protokołu odbioru w miejscu instalacji urządzeń,
2. możliwość zgłaszania usterki/awarii systemu 24h 7 dni w tygodniu,
3. usunięcie usterki/awarii systemu 24h od chwili zgłoszenia awarii,
4. wykonanie aktualizacji oprogramowania układowego lub innego oprogramowania wchodzącego w skład systemu w przypadku zaleceń producenta oferowanego systemu,
5. cała obsługa serwisu gwarancyjnego musi odbywać się w języku polskim,
6. wsparcie techniczne w okresie gwarancyjnym świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub polskiego partnera serwisowego producenta, obejmujące wymianę uszkodzonego urządzenia, bieżącą pomoc w konfiguracji systemu, dostęp do nowych wersji oprogramowania systemu, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

IV Miejsce instalacji:

1. Kraków, ul. Józefa 21.
2. Kraków, ul. Racławicka 56a.