**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**WPROWADZENIE**

Przedmiotem zamówienia jest **Zakup i dostawa oprogramowania systemu realizującego monitorowanie, kontrolę, rejestrację i audyt zdalnych sesji administracyjnych.**

Oprogramowanie do zarządzania dostępem uprzywilejowanym należy:

* dostarczyć w najnowszej dostępnej wersji do siedziby Zamawiającego,
* udzielić lub zapewnić udzielenie wieczystej licencji dla oprogramowania na warunkach producenta,
* wdrożyć dostarczony System w środowisku Zamawiającego,
* przeprowadzić instruktaż dla personelu Zamawiającego z wdrożenia i administracji Systemem,

Wykonawca zapewni, że przedmiot umowy odpowiada warunkom zawartym w Specyfikacji Warunków Zamówienia.

**Szczegółowy zakres minimalnych parametrów technicznych i funkcjonalności oprogramowania**

|  |  |  |
| --- | --- | --- |
| **LP** | **NAZWA ZAKUPU** | **OPIS** |
| **1** | **Narzędzie do zarządzania dostępem uprzywilejowanym** | **Wymagania ogólne*** Rozwiązanie w postaci oprogramowania z możliwością instalacji w środowisku VMvare Zamawiającego
* Rozwiązanie typu „solution in a box” – nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej ani zakupu dodatkowych licencji systemu operacyjnego.
* Rozwiązanie umożliwia rejestrację i zarządzanie dostępem uprzywilejowanym z wykorzystaniem protokołów opisanych w kolejnych punktach, do min. **100** serwerów, przy czym przez serwer rozumie się unikatowy adres IP wraz z protokołem komunikacji
* Rozwiązanie składa się co najmniej z następujących modułów:
	+ modułu zarządzania i rejestracji sesji uprzywilejowanych – funkcjonalność Session Manager,
	+ modułu zarządzania hasłami kont na zdefiniowanych serwerach – min. dla systemów WIndows, Windows Server i systemach z rodziny Unix (Linux Red Hat, Linux Suse, Linux Debian, Linux Ubuntu, FreeBSD 10+) oraz baz danych MySQL – funkcjonalność Password Manager,
* Rozwiązanie pozwala na monitorowanie i rejestrację protokołów:
	+ graficznych:
		- RDP – włączając w to sesje wielomonitorowe
		- VNC
	+ tekstowych:
		- SSH
		- telnet
	+ **aplikacyjnych:**
		- **HTTP/HTTPS**
* W zakresie obsługi protokołu RDP rozwiązanie musi umożliwić połączenie z wykorzystaniem:
	+ sesji szyfrowania TLS
	+ sesji szyfrowania TLS z uwierzytelnieniem NLA
	+ sesji nieszyfrowanej
* W zakresie obsługi protokołu SSH rozwiązanie musi oferować:
	+ obsługę podsystemu SFTP – przegląd i pobieranie przesłanych plików
	+ obsługę tunelu X11
* Rozwiązanie musi umożliwiać rozpoczęcie i realizację sesji zarówno przez wywołanie połączenia z poziomu aplikacji realizującej dany protokół (aplikacja zainstalowana na urządzeniu klienckim) jak i z poziomu przeglądarki internetowej, poprzez stronę uruchomienie połączenia z danym protokołem za pomocą aplikacji wspomagającej obsługującej dany protokół – przynajmniej dla protokołów RDP i SSH
	+ funkcja rozpoczęcia sesji poprzez przeglądarkę internetową musi być dostępna tylko dla użytkowników, którzy przed tym poprawnie się uwierzytelnią
	+ powyższe uwierzytelnienie musi być możliwe także dla użytkowników zdefiniowanych w zewnętrznym katalogu – przynajmniej Active Directory i Radius
* Rozwiązanie umożliwia podgląd i zarządzanie sesjami “na żywo”, tzn. niezakończonymi:
	+ w ramach tego podglądu musi być możliwość dołączenia do sesji – przynajmniej dla protokołów RDP, VNC, SSH
	+ operator przeglądający sesję “na żywo” musi mieć możliwość natychmiastowego rozłączenia sesji i blokowania użytkownika (niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników)
* Administracja, monitorowanie oraz podgląd zapisanych w rozwiązaniu sesji odbywa się poprzez przeglądarkę WWW
* W rozwiązaniu analiza i rejestracja sesji dla ww. protokołów odbywa się wyłącznie na urządzeniu; nie dopuszcza się stosowania tzw. „stacji przesiadkowych”
* Rozwiązanie musi umożliwić podanie przez nawiązującego sesję powodu jej rozpoczęcia i zapisywać wprowadzony tekst w metadanych sesji, wprowadzenie tekstu musi być realizowane przed nawiązaniem sesji do serwera (systemu) docelowego

- na potrzeby inwentaryzacji * Rozwiązanie pozwala na kontrolę i ograniczenie właściwości sesji protokołowych:
	+ dla protokołu RDP minimum:
		- ograniczenie maksymalnej rozdzielczości ekranu sesji
		- ograniczenie głębi kolorów, min. do 8 i 16 bpp
		- blokowanie funkcji schowka
	+ dla protokołu SSH minimum:
		- blokowanie przekazywania portów (port forwarding)
		- blokowanie tunelu X11
		- blokowanie przekazywania agenta SSH
		- blokowanie podsystemu SFTP i przesyłania plików z wykorzystaniem scp
* Rozwiązanie posiada możliwość uwierzytelniania poprzez zewnętrzne serwery: Active Directory, Radius
* Rozwiązanie umożliwia synchronizację użytkowników z Active Directory, w tym:
	+ z wybranymi grupami w domenie Active Directory
	+ tylko w zakresie danej lub danych organizacji (OU)
	+ z kilkoma domenami Active Directory
	+ z użytkownikami i grupami wskazanymi na podstawie zdefiniowanego filtru
* Rozwiązanie nagrywa cały ruch sieciowy związany z daną sesją (rejestracja surowego protokołu)
* Rozwiązanie pozwala na selektywne wskazanie systemów, dla których ma być włączone nagrywanie sesji
* Rozwiązanie umożliwia podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym
* Dla sesji graficznych rozwiązanie umożliwia uruchomienie własnego ekranu logowania przed nawiązaniem połączenia z serwerem (systemem) docelowym
* Rozwiązanie posiada możliwość wymuszenia akceptacji operatora przed nawiązywaniem sesji
* Rozwiązanie umożliwia automatyczne przerwanie sesji po wykryciu wcześniej zdefiniowanego ciągu znaków oraz alert administratora
* Rozwiązanie umożliwia przeszukiwanie sesji w trybie pełnotekstowym
	+ wyszukiwanie musi być możliwe zarówno dla kanału wejściowego (np. wpisywane komendy) jak i danych wyjściowych, pojawiających się na ekranie nawiązanej sesji
	+ powyższe dotyczy to także sesji graficznych w protokołach RDP i VNC, a co za tym idzie wszystkich treści pojawiających się na ekranie
	+ możliwość wyszukiwania musi być natychmiastowa, z wyjątkiem sesji graficznych, dla których dopuszcza się zastosowanie mechanizmu indeksującego OCR
	+ przygotowanie sesji do wyszukiwania musi być realizowane wewnętrznie, tzn. dane nie mogą być wysyłane do chmury lub innego dedykowanego urządzenia
	+ funkcja wyszukiwania musi być możliwa do wyłączenia przynajmniej dla wskazanego użytkownika na serwerze
* Rozwiązanie umożliwia udzielenie czasowego dostępu do pojedynczej sesji – zarówno zakończonej i zapisanej jak niezakończonej („na żywo”)
	+ w ramach sesji niezakończonej („na żywo”) operator musi mieć możliwość określenia czy sesja ma być udostępniona tylko w trybie podglądu czy z możliwością dołączenia do sesji
	+ musi być możliwość wycofania udzielonego dostępu do współdzielonej sesji w każdej chwili
* Rozwiązanie musi mieć możliwość definiowania hierarchii użytkowników i operatorów, co najmniej w zakresie:
	+ zwykłego konta użytkownika
	+ konta operatora z dostępem do przeglądu
	+ konta operatora z możliwością przeglądu konfiguracji
	+ konta operatora z możliwością zmiany konfiguracji
	+ konta operatora z możliwością zarządzania systemem (np. restart urządzenia)
* Rozwiązanie musi umożliwić zdefiniowanie polityki retencji sesji, tj. okresu, po którym sesje będą kasowane z urządzenia
* Rozwiązanie musi umożliwić zdefiniowanie zestawu komend lub ciągów znaków, których wprowadzenie w trakcie trwania sesji lub pojawienie się w treści sesji wywoła zdefiniowane przez operatora działanie, co najmniej:
	+ informacja wysłana do operatora poprzez e-mail
	+ natychmiastowe zakończenie rozpoczętej sesji z możliwością automatycznego zablokowania konta użytkownika niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników
	+ zatrzymanie rozpoczętej sesj
	+ zestaw komend lub ciągów znaków musi być możliwy do zdefiniowania z wykorzystaniem mechanizmu wyrażeń regularnych (regexp) przy czym mechanizm wildcard nie będzie uznany za równoważny
* Rozwiązanie musi umożliwiać zapisanie sesji w postaci nagrania wideo
* Rozwiązanie musi wspierać zmianę haseł w systemach Unix za pomocą uprzywilejowanego konta z dostępem z wykorzystaniem klucza SSH
* Rozwiązanie umożliwia zdefiniowanie złożoności automatycznie generowanych haseł

- na potrzeby audytowe, ze względów bezpieczeństwa * Rozwiązanie zapewnia ochronę kryptograficzną wszystkich zapisanych danych (szyfrowanie oraz integralność) na poziomie bezpieczeństwa nie gorszym niż poziom gwarantowany przez szyfr AES256. Producent rozwiązania nie może mieć możliwość odszyfrowania zapisywanych na urządzeniu danych bez dostępu do oryginalnych kluczy szyfrujących (brak tzw. “kluczy serwisowych”)
* Rozwiązanie musi umożliwić zdefiniowanie własnego certyfikatu / klucza dla połączeń szyfrowanych (dla protokołów RDP i SSH) jak również przeniesienie istniejących certyfikatów / klucza z serwera (systemu), do którego dostęp jest zdefiniowany – obsługa fraz szyfrujących certyfikat / klucz
* Rozwiązanie musi umożliwić weryfikację certyfikatu / klucza serwera (systemu), do którego dostęp jest zdefiniowany – przynajmniej dla protokołów RDP i SSH
* Rozwiązanie musi umożliwić podstawową diagnostykę sieciową:
	+ potwierdzenie komunikacji za wykorzystaniem sygnalizacji ICMP (ping)
	+ potwierdzenie komunikacji z wykorzystaniem połączenia TCP (połączenie z dowolnym portem dowolnego adresu IP)
* Rozwiązanie musi zawierać wszystkie niezbędne licencje do uruchomienia wyżej opisanej funkcjonalności. Rozwiązanie musi być objęte licencją dożywotnią.
* System musi być objęty trzyletnim wsparciem serwisowym producenta i musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Po zakończeniu wsparcia serwisowego producenta, system nie może stracić swojej funkcjonalności.
* Wymagane jest zapewnienie technicznego wsparcia w przez telefon, e-mail i stronę WWW w trybie 8x5 przez okres co najmniej trzech lat.
* Rozwiązanie musi umożliwić wprowadzenie znakowania czasowego do zapisu sesji przez podmioty kwalifikowane (co najmniej przez KIR i PWPW)

Kryteria pozacenowe:* Dostarczony system zarządzania dostępem uprzywilejowanym zawiera dodatkowy moduł raportowania aktywności i wydajności w ramach zarejestrowanych sesji, umożliwiający co najmniej wygenerowanie raportów zawierających informacje pozwalające określić czas rzeczywistej aktywności użytkownika (czas, w którym wykonywane były działania, użytkownik wykonywał prace) w stosunku do całościowego czasu trwania sesji – 10%
* Dostarczony system zarządzania dostępem uprzywilejowanym nie wymaga instalowania dodatkowego oprogramowania (agentów) ani na monitorowanych serwerach, ani na stacjach klienckich, z których wykonywane są połączenia. – 10%
* Rozwiązanie posiada dokumentację, interfejs użytkownika oraz wsparcie techniczne w języku polskim – 10%
* Rozwiązanie umożliwia wprowadzenie konieczności dodatkowej akceptacji połączenia uprzywilejowanego przez nadzorcę (osobę trzecią) po poprawnym uwierzytelnieniu się użytkownika – 10%
 |