**Opis przedmiotu zamówienia**

1. **W ramach realizacji przedmiotu zamówienia Wykonawca:**
	1. Dostarczy system zarządzania dostępem uprzywilejowanym i przeniesienie na rzecz Zamawiającego własność urządzeń - rozwiązanie musi być dostarczone z platformą sprzętową pracującą w kastrze.
	2. Udzieli lub zapewni udzielenie niezbędnych licencji do prawidłowego działania Systemu jak również do korzystania z wszystkich funkcjonalności określonych przez Zamawiającego. Dostarczone licencje muszą być nadane bezterminowo.
	3. Zapewni licencje na System, uprawniające do:
2. zarządzania (w zakresie haseł, haseł w skryptach, kluczy) przez oferowane rozwiązanie systemami docelowymi Zamawiającego, w liczbie nie mniejszej niż 100;
3. korzystania z oferowanego rozwiązania przez użytkowników w liczbie nie mniejszej niż 50,
4. administrowania systemem przez operatorów (administratorów) w liczbie nie mniejszej niż 5.
	1. Opracuje projekt wdrożeniowy zgodnie z wymaganiami Zamawiającego obejmujący instalację, konfigurację systemu i integrację z systemami obecnie funkcjonującymi u Zamawiającego oraz wykona dokumentację powykonawczą.
	2. Zainstaluje, uruchomi i dokonana konfiguracji wszystkich urządzeń i oprogramowania zgodnie z minimalnymi wymaganiami określonymi w pkt 8 jak również w oparciu o założenia projektu wdrożeniowego.
	3. Przeprowadzi szkolenie administratorów zaoferowanego Systemu z zakresu administrowania dostarczonego systemu zgodnie z wymaganiami określonymi w pkt. 6.
	4. Przeprowadzi szkolenie użytkowników zaoferowanego systemu z zakresu funkcjonowania i obsługi zgodnie z wymaganiami określonymi w pkt. 7.
	5. Zapewni co najmniej 36 miesięczny okresu gwarancji i serwisu.
	6. Zapewni usługi konsultacyjne w ilości co najmniej 180 godzin do wykorzystania od momentu podpisania protokołu odbioru.

**2. Architektura sytemu**

1. System musi zapewniać wysoką dostępność i niezawodność poprzez zastosowanie wdrożenia klastrowego – dwa serwery skonfigurowane co najmniej w modelu Active-Passive z automatycznym przełączeniem urządzeń w przypadku awarii jednego z nich. W ramach tych serwerów musi być zainstalowana całość oprogramowania obejmująca system operacyjny, bazę danych, oprogramowanie, które będzie realizowało pełną funkcjonalność Systemu w trybie wysokiej dostępność. Serwery muszą zapewnić redundancję na poziomie zasilania oraz dysków wewnętrznych.
2. Serwery będą zainstalowane w dwóch różnych lokalizacjach (budynkach).
3. Wszystkie zaoferowane przez Wykonawcę komponenty rozwiązania w całości będą pochodzić od jednego producenta/wytwórcy oprogramowania (platforma serwerowa i oprogramowanie).
4. Fizyczne serwery muszą spełniać następujące minimalne parametry:
5. wysokość maksimum 2U,
6. 4 interfejsy sieciowe 10Gbit SFP+.
7. System musi zapewnić możliwość wykonania i odtworzenia całości i/lub części Systemu z kopii bezpieczeństwa w przypadku awarii jednego węzła oraz ma narzędzia do wykonywania kopii bezpieczeństwa konfiguracji, która umożliwia odtworzenie całego Systemu w przypadku awarii obu węzłów klastra jednocześnie.
8. System nie może wymagać instalowania dodatkowego oprogramowania (agentów) ani na monitorowanych serwerach ani na stacjach klienckich, z których wykonywane są połączenia.
9. System musi mieć możliwość rozbudowy o światłowodowe interfejsy sieciowe pracujące w standardzie 802.1ae z wykorzystaniem interfejsów 10GBASE-SX i -LX i złącz SFP+.
10. System musi zapewniać 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”).
11. System musi posiadać przestrzeń dyskową na dane (użytkową) umożliwiającą rejestrację i przechowywanie gromadzonych danych (monitorowanych sesji) przez okres minimum 2 lat licząc dla sesji RDP, przy założeniu przechowywania minimum 50 sesji RDP dziennie, gdzie jedna sesja trwa średnio 8 godzin dziennie i jest uruchamiana przez 365 dni w roku.
12. System musi posiadać wydajność umożliwiającą jednoczesną rejestrację do min. 50 sesji tekstowych (dla protokołów SSH lub telnet) lub min. 25 sesji (dla protokołów RDP lub VNC) – liczone dla pojedynczego urządzenia lub dla klastra z aktywnym tylko jednym węzłem.
13. **System musi posiadać następujące cechy i funkcjonalności**
14. System musi posiadać interfejs użytkownika w całości w języku polskim (zarówno w panelu administratora systemu jak i panelu użytkownika).
15. Interfejs systemu musi być dostępny w bezpiecznym połączeniu za pośrednictwem przeglądarki internetowej.
16. System musi posiadać wsparcie dla zarządzania kontami uprzywilejowanymi dla:

a) Systemów operacyjnych: Windows Server od wersji 2003, Windows Desktop od wersji 7, Linux dystrybucje z 2015 roku i późniejsze,

b) Baz danych: MySQL, SQL Server,

c) Urządzeń: Cisco.

1. System musi dawać możliwość definiowanie polityk złożoności hasła w zakresie jego długości oraz zawartości (duże litery, małe litery, cyfry, znaki specjalne).
2. System musi generować hasła automatycznie dla kont systemów docelowych zgodnie ze zdefiniowaną polityką złożoności haseł.
3. System musi automatycznie zmieniać hasła na wskazanych kontach systemów docelowych zgodnie ze zdefiniowaną polityką częstotliwości zmiany hasła.
4. System musi umożliwia ręczną (inicjowaną przez administratora) zmianę hasła na wskazanym koncie systemu docelowego.
5. System musi zapewniać funkcjonalność umożliwiającą zmianę hasła na koncie systemu docelowego po zakończeniu połączenia z tym systemem.
6. W przypadku systemów Windows zmianie musi podlegać także hasło w usługach które korzystają z konta dla którego hasło zostało automatycznie zmienione.
7. System musi umożliwiać weryfikację czy hasło nie zostało zmienione w sposób nieuprawniony.
8. System musi zapewniać weryfikację zgodności hasła na koncie systemu docelowego z hasłem zapisanym w Systemie ze zdefiniowaną częstotliwością (codziennie, tygodniowo, miesięcznie).
9. System musi umożliwiać podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym.
10. System musi przechowywać historię haseł do kont i umożliwiać odzyskanie wybranego hasła.
11. Dla sesji graficznych i tekstowych (przynajmniej dla SSH i telnet) System musi umożliwić połączenie z serwerem (systemem) bez znajomości ani nazwy domenowej (FQHN) ani adresu IP tego serwera (systemu), a jedynie nazwy zdefiniowanej przez operatora;.
12. System musi mieć wbudowane mechanizmy rozliczalności, uwierzytelnienia i autoryzacji.
13. System musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez różne lub jedno konto uprzywilejowane.
14. Funkcjonalność monitoringu sesji realizowana przez System musi umożliwiać informowanie operatora co najmniej o następujących o zdarzeniach:
15. rozpoczęcia sesji,
16. zakończenia sesji,
17. rozłączenia się takiego operatora lub osoby.
18. Ww. funkcja musi być realizowana przynajmniej z wykorzystaniem protokołu syslog i poprzez e-mail.
19. System musi pozwalać na monitorowanie i rejestrację protokołów:
20. graficznych: RDP – włączając w to sesje wielomonitorowe i VNC,
21. tekstowych: SSH i telnet – dopuszcza się konieczność podwójnego uwierzytelnienia (ograniczenie protokołu),
22. aplikacyjnych: HTTP/HTTPS, MySQL, MS SQL i innych, opartych o konektor TDS, Oracle – może być realizowane przez tzw. RemoteApp
23. W zakresie obsługi protokołu RDP System musi umożliwić połączenie z wykorzystaniem:
24. sesji szyfrowania TLS,
25. sesji szyfrowania TLS z uwierzytelnieniem NLA ,
26. W zakresie obsługi protokołu SSH System musi oferować obsługę tunelu X11.
27. System musi umożliwiać rozpoczęcie sesji zarówno przez wywołanie połączenia z poziomu aplikacji realizującej dany protokół jak i z poziomu przeglądarki internetowej, poprzez stronę – uruchomienie połączenia z danym protokołem za pomocą aplikacji wspomagającej obsługującej dany protokół – przynajmniej dla protokołów RDP (plik typu „.rdp) i SSH (odnośnik ssh://):
28. funkcja rozpoczęcia sesji poprzez przeglądarkę internetową musi być dostępna tylko dla użytkowników, który przed tym poprawnie się uwierzytelnią,
29. powyższe uwierzytelnienie musi być możliwe także dla użytkowników zdefiniowanych w zewnętrznym katalogu – przynajmniej Active Directory, LDAP.
30. System musi umożliwiać podgląd i zarządzanie sesjami “na żywo”, tzn. niezakończonymi z poziomu przeglądarki internetowej i umożliwić operatorowi:
31. natychmiastowe rozłączenia sesji i blokowania użytkownika (niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników),
32. zatrzymanie sesji bez jej rozłączania i wznowienia jej w dowolnym momencie
33. Administracja, monitorowanie oraz podgląd zapisanych w rozwiązaniu sesji odbywa się poprzez przeglądarkę WWW.
34. Podgląd monitorowanych sesji, zarówno “na żywo” jak i wcześniej nagranych, nie wymaga instalowania dodatkowego oprogramowania (dotyczy także wtyczek do przeglądarek, np. Flash).
35. System musi posiadać możliwość wymuszenia akceptacji operatora przed nawiązywaniem sesji.
36. System musi umożliwić podanie przez nawiązującego sesję powodu jej rozpoczęcia i zapisywać wprowadzony tekst w metadanych sesji:
37. wprowadzenie ww. tekstu musi być realizowane przed nawiązaniem sesji do serwera (systemu) docelowego,
38. wprowadzenie ww. tekstu musi być realizowane co najmniej dla protokołów: RDP, VNC, SSH, telnet.
39. System musi posiadać możliwość uwierzytelniania poprzez zewnętrzne serwery: Active Directory, Radius, LDAP (w tym OpenLDAP).
40. System musi umożliwiać synchronizację użytkowników z Active Directory, w tym:
41. z wybranymi grupami w domenie Active Directory, w tym z grupami zawierającymi inne grupy,
42. tylko w zakresie danej lub danych organizacji (OU),
43. z kilkoma domenami Active Directory – także w sytuacji, gdy nazwy użytkowników w domenach się powtarzają w dwóch lub więcej domenach,
44. z użytkownikami i grupami wskazanymi na podstawie zdefiniowanego filtru.
45. System musi posiadać możliwość definiowania hierarchii użytkowników i operatorów, co najmniej w zakresie:
46. zwykłego konta użytkownika,
47. konta operatora z możliwością przeglądu konfiguracji,
48. konta operatora z możliwością zmiany konfiguracji,
49. konta operatora z możliwością zarządzania systemem (np. restart urządzenia).
50. System musi posiadać możliwość ograniczenia dostępu operatora do najmniej:
51. wskazanych serwerów (systemów) oraz zapisanych i trwających do nich sesji,
52. wskazanych użytkowników oraz zapisanych i trwających sesji tychże.
53. System musi pozwalać na selektywne wskazanie systemów, dla których ma być włączone nagrywanie sesji.
54. System musi umożliwiać zapisanie zakończonej sesji w postaci nagrania wideo w formacie umożliwiającym odtworzenie nagrania za pomocą programu VLC w wersji 3.0 lub nowszej – zapis taki musi być możliwy zarówno dla protokołów graficznych (przynajmniej VNC i RDP) jak i tekstowych (przynajmniej SSH i telnet).
55. System musi umożliwiać przeszukiwanie sesji w trybie pełnotekstowym:
56. wyszukiwanie musi być możliwe zarówno dla kanału wejściowego (np. wpisywane komendy) jak i danych wyjściowych, pojawiających się na ekranie nawiązanej sesji,
57. przygotowanie sesji do wyszukiwania musi być realizowane wewnętrznie, tzn. dane nie mogą być wysyłane do chmury lub innego dedykowanego urządzenia.
58. System musi umożliwiać zdefiniowanie polityki retencji sesji, tj. okresu, po którym sesje będą kasowane z urządzenia – musi istnieć możliwość zdefiniowania innej polityki retencji.
59. System musi posiadać możliwość integracji z zewnętrznym repozytorium haseł innego producenta niż oferowany System np. CyberArk.
60. System musi wspierać uwierzytelnienie jednorazowym hasłem w standardzie zgodnym z co najmniej RFC 4226 (HOTP) i RFC 6238 (TOTP) – zarówno jako hasło główne jak i w konfiguracji, gdy hasło jednorazowe stanowi drugi składnik uwierzytelnienia (pierwszym jest hasło statyczne lub hasło domeny AD lub LDAP)..
61. System musi umożliwiać zarządzanie skryptowe z wykorzystaniem API umożliwiającego co najmniej:
62. tworzenie, zmianę i usuwanie kont użytkowników,
63. tworzenie, zmianę i usuwanie serwerów (systemów docelowych),
64. tworzenie, zmianę i usuwanie dostępu do ww. serwerów (systemów) – dotyczy kont na tychże,
65. tworzenie, zmianę i usuwanie adresów IP i portów, do których będą się łączyć użytkownicy,
66. tworzenie, zmianę i usuwanie relacji między kontami, serwerami, dostępami,
67. pobieranie listy sesji – z możliwością rozróżnienia sesja, które nie zostały jeszcze zakończone,
68. blokowanie użytkownika – niezależnie od stanu użytkownika wynikającego z synchronizacji z zewnętrznymi zbiorami użytkowników.
69. System musi umożliwiać 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.
70. System musi umożliwiać weryfikację certyfikatu/klucza serwera (systemu), do którego dostęp jest zdefiniowany – przynajmniej dla protokołów RDP i SSH – w przypadku protokołu RDP musi być możliwość weryfikacji certyfikatu serwera (systemu) docelowego na podstawie zdefiniowanego w urządzeniu (zaimportowanego) certyfikatu CA.
71. System musi umożliwiać monitorowanie wybranych parametrów pracy z wykorzystaniem protokołu SNMP w wersji min. V3.
72. System musi umożliwiać podstawową diagnostykę sieciową: potwierdzenie komunikacji za wykorzystaniem sygnalizacji ICMP (ping), potwierdzenie komunikacji z wykorzystaniem połączenia TCP (połączenie z dowolnym portem dowolnego adresu IP).
73. System musi współpracować z usługami sieciowymi: NTP, - name server (DNS).
74. System musi współpracować z systemami klasy SIEM – przynajmniej z wykorzystaniem protokołu syslog.
75. System musi posiadać zaimplementowane oznakowanie komunikatów systemowych wysyłanych do systemu SIEM (tagowanie) umożliwiające kategoryzację wydarzeń w takim systemie.
76. System musi zawierać wszystkie niezbędne licencje do uruchomienia wyżej opisanej funkcjonalności, włączając w licencje na system operacyjny – jeżeli takie są niezbędne do jej uruchomienia.

**4. Zamawiający dopuszcza posiadanie przez Systemem funkcjonalności, które nie są wymagane przez Zamawiającego lecz mogą stanowić dodatkową funkcjonalność Systemu ocenianą przez Zamawiającego w kryteriach oceny ofert.** **Funkcjonalności dodatkowe które zamawiający będzie brał pod uwagę przedstawia poniższa tabela:**

|  |  |  |
| --- | --- | --- |
| 4.1 | Automatyczne rozpoznawania (skanowania) kont uprzywilejowanych na poniżej wymienionych zasobach: • konta linux/unix• lokalne konta systemu Windows• zasoby w domenie Active Directory • konta Vmware ESX/ESXi | Spełnia/nie spełnia\* |
| 4.2 | Posiadanie mechanizmu OCR, który musi być realizowany co najmniej dla sesji HTTP/HTTPS (zarówno w postaci tekstowej jak i graficznej), VNC oraz RDP poprzez rozpoznawanie i zapisanie w bazie danych wszystkich znaków i tekstów które były wyświetlone w sesji; dotyczy to zarówno tekstów (poleceń) wprowadzonych na klawiaturze jak również znaków i tekstów, które ukazały się w dowolnym miejscu ekranu sesji graficznej (okna aplikacji, dane edytowanych dokumentów, „wyskakujące” okna powiadomień, nazwy plików, itd.) OCRFunkcja wyszukiwania musi być możliwa do wyłączenia przynajmniej dla wskazanego użytkownika na serwerze. | Spełnia/nie spełnia\* |

**\* - niepotrzebne skreślić**

**5. Minimalne wymagania Zamawiającego dotyczące wytwarzanych i przetwarzanych dokumentów w tym dokumentacji powykonawczej**

1. Wykonawca przygotuje dokumentację powykonawczą szczegółowo opisującą wszystkie zrealizowane prace instalacyjne i konfiguracyjne wraz ze schematem podłączenia Systemu w infrastrukturze Zamawiającego.
2. W ramach dokumentacji powykonawczej Wykonawca dostarczy procedury i instrukcje administracyjne, obejmujące w szczególności:
3. wykonanie kopii bezpieczeństwa Systemu i jego odtworzenie,
4. aktualizację i wdrażania poprawek,
5. procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,
6. diagnozowanie systemu i jego komponentów,
7. sprawdzanie wydajności poszczególnych komponentów system,
8. sprawdzanie poprawności działania trybu wysokiej dostępności wdrożonego Systemu,
9. konfigurację: kont użytkowników, dodawania systemów, podglądu/haseł, tworzenia nowych połączeń, zmiany harmonogramu rotacji haseł,
10. konfigurację parametrów nagrywania sesji,
11. instrukcję obrazkową z opisem wstrzykiwania wtyczki z systemu PAM do nowo zakupionego serwera
12. Każda z procedur powinna zawierać co najmniej następujące dane:
	1. nazwa,
	2. opis,
	3. częstotliwość wykonywania,
	4. kroki do zrealizowania w procedurze,
	5. informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce) na jakie należy zwrócić uwagę w trakcie wykonywania procedury,
	6. omówienie zawartości komunikatów jeśli są prezentowane,
	7. kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.
13. Dokumentacja musi być weryfikowana i w razie potrzeby aktualizowana podczas prac serwisowych Wykonawcy.
14. Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji.

**6. Minimalne wymagania stawiane przez Zamawiającego w zakresie szkolenia administratorów:**

1. Wykonawca zorganizuje szkolenie z wdrożonego Systemu, dla jednej grupy administratorów, składającej się maksymalnie z 5 osób, w ośrodku szkoleniowym producenta lub Wykonawcy na terenie Warszawy, lub w siedzibie Zamawiającego.
2. Termin i miejsce szkolenia zostanie uzgodnione z Zamawiającym z co najmniej tygodniowym wyprzedzeniem.
3. Szkolenie musi trwać minimum 2 dni robocze, 6 godzin dziennie efektywnych zajęć prowadzonych w języku polskim.
4. Szkolenie musi być prowadzone przez certyfikowanego inżyniera Wykonawcy lub producenta zaoferowanego systemu.
5. Program szkolenia musi być zgodny z wykorzystywaną przez Zamawiającego wersją systemu oraz obejmować całość zagadnień związanych z czynnościami administracyjnymi zaoferowanego systemu w tym:
6. konfiguracja,
7. zarządzanie,
8. monitorowanie,
9. raportowanie,
10. omówienie najczęściej występujących awarii oraz sposoby ich usuwania i zabezpieczania się przed nimi.

**7. Minimalne wymagania stawiane przez Zamawiającego w zakresie szkoleń użytkowników**

1. Wykonawca zorganizuje szkolenie z wdrożonego Systemu, dla grupy użytkowników składającej się maksymalnie 10 osób, w ośrodku szkoleniowym producenta lub Wykonawcy na terenie Warszawy, lub w siedzibie Zamawiającego.
2. Termin i miejsce szkolenia zostanie uzgodnione z Zamawiającym z co najmniej tygodniowym wyprzedzeniem.
3. Szkolenie musi trwać minimum 1 dzień roboczy, 6 godzin dziennie efektywnych zajęć prowadzonych w języku polskim.
4. Szkolenie musi być prowadzone przez certyfikowanego inżyniera Wykonawcy lub producenta zaoferowanego systemu.
5. Program szkolenia musi być zgodny z wykorzystywaną przez Zamawiającego wersją systemu oraz obejmować całość zagadnień związanych z czynnościami administracyjnymi zaoferowanego systemu w tym:
6. obsługa interfejsu programu,
7. zarządzanie własnymi ustawieniami (profilu użytkownika), połączeniami.

**8. Minimalne wymagania w trakcie wdrożenia**

1. Instalacja Systemu w infrastrukturze Zamawiającego wraz z konfiguracja wysokiej dostępności (klasterActive-Passive lub replikacja typu Disaster Recovery)
2. Konfiguracja i parametryzacja poszczególnych komponentów systemu.
3. Konfiguracja kont użytkowników oraz połączeń do systemów docelowych (SSH, RDP, WWW) wraz uprawieniami dla wybranych użytkowników i automatyczną zmianą hasła na systemie docelowym.
4. Konfiguracja kont użytkowników jak i połączeń do systemów docelowych rozumiana jest przez Zamawiającego jako możliwość połączenia co najmniej 30 użytkowników do 50 systemów (adresów IP) przy założeniu że na każdym adresie IP może działać więcej niż 1 usługa, np. SSH i WWW lub RDP i WWW, przy założeniu że dostęp do tych usług może odbywać się równolegle.
5. Konfiguracja konieczności akceptacji dostępu do wybranych systemów przez użytkowników.

**9. Inne**

1. Do urządzeń muszą zostać dostarczone wszelkiego rodzaju uchwyty, mocowania, śruby, przewody umożliwiające instalację urządzenia w szafie RACK i podłączenia go do sieci elektrycznej i informatycznej Zamawiającego.
2. Instalacja, uruchomienie, konfiguracja i integracja z infrastrukturą zamawiającego należy wykonać w okresie realizacji zamówienia, w dni robocze, w godzinach 8:15-16:15. W siedzibie Komendy Głównej Państwowej Straży Pożarnej przy ul. Podchorążych 38, w Warszawie (00 463).
3. Prowadzenie prac na infrastrukturze Zamawiającego wymaga spełnienia wymagań procedury dostępu do usług teleinformatycznych Zamawiającego (wypełnienie wniosku) i uzyskanie formalnej zgody Zamawiającego), a także zachowania najwyższej staranności w celu ochrony Infrastruktury Zamawiającego przed możliwym naruszeniem jej bezpieczeństwa;

……………………………..…………………………..

data, imię i nazwisko, podpis osoby uprawnionej