**SI-II.2601.109.2019**

**Szczegółowy opis przedmiotu zamówienia na dostawę licencji na system do nadzorowania sesji zdalnych.**

Wymagania podstawowe.

|  |  |
| --- | --- |
| 1. | Rozwiązanie powinno działać jako PROXY, bez potrzeby instalacji przez administratora agentów na systemach chronionych rozwiązaniem PAM. |
| 2. | Rejestracja i podgląd sesji uprzywilejowanych użytkowników (polecenia i zrealizowane działania) umożliwiając funkcje bezpieczeństwa niezaprzeczalności wykonanych działań i zabezpieczenie materiału dla celów sądowych. |
| 3. | Rozwiązanie powinno wspierać platformę wirtualną Microsoft Hyper-V lub VMware z możliwością bezpłatnego, z punktu widzenia licencji, migrowania systemu z jednej platformy na drugą. |
| 4. | Rozwiązanie powinno wspierać natywnie połączenia dla protokołów SSH i RDP do PROXY oraz SSH/TELNET/RLOGIN/RDP/VNC od PROXY do systemów chronionych. |
| 5. | Dla niestandardowych protokołów (nie wspieranych natywnie przez rozwiązanie dostawcy) powinna istnieć możliwość wywołania klienta, wspierającego taki protokół, na stacji przesiadkowej, w taki sposób, aby jedynie klient i przypisane mu zasoby były widoczne dla użytkownika. |
| 6. | Dla niestandardowych protokołów i wywołania ich klienta, rozwiązanie powinno wspierać technologie Microsoft RemoteApp. |
| 7. | Możliwość przydzielania uprawnień administracyjnych oraz dostępowych dla użytkowników na podstawie profili ustawień. |
| 8. | W przypadku dostępu audytora profil użytkownika powinien co najmniej oferować możliwość ograniczenia dostępu do nagrań wybranych grup użytkowników i grup systemów docelowych wraz z konfigurowanymi dla nich kontami uprzywilejowanymi. |
| 9. | Konfiguracja profilu użytkownika powinna zawierać możliwość filtrowania połączeń przychodzących w oparciu o adres źródłowy IP. Tworząc tym samym listy kontroli dostępu (ACL) dla użytkowników z przypisanym profilem użytkownika. Definicja ograniczenia powinna dopuszczać format: adres IP, adres sieci i maska sieci lub FQDN. |
| 10. | Rozwiązanie powinno pozwalać na określenie polityki dostępu przez przypisanie wybranej grupie użytkowników do wskazanej grupy systemów docelowych. |
| 11. | Podgląd zarejestrowanych danych musi uwzględniać zapis video sesji oraz transkrypcje nagrania przedstawiającą wszystkie metadane dotyczące sesji (RDP) oraz pełny zapis wyświetlanych danych dla konsoli (SSH). |
| 12. | Monitorowanie połączeń w czasie rzeczywistym, w tym możliwość podglądu sesji w czasie rzeczywistym z możliwością jej natychmiastowego zakończenia. |
| 13. | Zarządzanie zbiorami reguł (polityką) haseł lokalnych użytkowników i administratorów. |
| 14. | Możliwość włączenia/wyłączenia rejestrowania sesji dla wybranych grup użytkowników. |
| 15. | Możliwość ustawienia dostępu przez portal internetowy, przeglądarkę, co najmniej dla sesji SSH i RDP, bez potrzeby instalacji dedykowanej wtyczki w przeglądarce. |
| 16. | Rozwiązanie umożliwia integracje z Microsoft Active Directory bez potrzeby synchronizacji informacji o użytkownikach. To znaczy, że użytkownik Active Directory dodany do grupy użytkowników automatycznie, w tej samej chwili jest rozpoznany przez rozwiązanie do zarządzania dostępem. |
| 17. | Możliwość definiowania systemów docelowych przez określenie adresu IP, nazwy DNS lub możliwość określania przez adres IP sieci i maski. |
| 18. | Dla sesji RDP „meta-dane” powinny zawierać informację na temat: a. zmiany aktywnego okna, b. operacji wyboru danego przycisku w oknie systemu Windows, c. operacji wyboru przycisków typu „radio button” lub zaznaczenie opcji typu „check box” w oknie, d. zmiany treści w polu tekstowym w oknie systemu Windows, e. rozpoczęcia i zakończenia procesu f. wymiany plików przez schowek systemu Windows, g. wymiany plików przez przekierowane zasoby sieciowe systemu Windows. |
| 19. | Identyfikacja na bazie meta-danych rozpoczęcia i zakończenia procesu nie może opierać się o OCR. |
| 20. | System powinien mieć możliwość znakowania czasem zapisanych sesji w oparciu o podstawę czasu serwera NTP. |
| 21. | Rozwiązanie musi umożliwiać zdefiniowanie polityk retencji dla nagrywanych sesji tj. okresu, po którym nagrane sesje będą kasowane. |
| 22. | System musi zapewniać współpracę z zewnętrzną przestrzenią dyskową w razie konieczności rozszerzenia podstawowej przestrzeni dyskowej poprzez integrację co najmniej z zastosowaniem protokołów CIFS oraz NFS. |
| 23. | Rozwiązanie powinno umożliwiać eksport konfiguracji (backup) w postaci zaszyfrowanej z określeniem dedykowanego klucza (hasła). Eksport konfiguracji powinno móc wykonać się zarówno z interfejsu użytkownika (GUI), jak i linii poleceń (CLI). |
| 24. | W przypadku wykonywania eksportu konfiguracji z linii poleceń (CLI) Systemu musi mieć możliwość definiowania częstotliwości wykonywania eksportu konfiguracji. |
| 25. | Dla sesji RDP możliwość blokowania połączeń TCP wychodzących na stacji docelowej, serwera Microsoft Windows. |
| 26. | Dla sesji RDP możliwość blokowania wybranych procesów na stacji docelowej, serwer Microsoft Windows. |
| 27. | Dla sesji SSH i RDP możliwość tworzenia wzorców regex dla wykonywanych poleceń, a w przypadku wykrycia takiego wzorca możliwość ustawienia jednej z akcji: zakończenie sesji lub powiadomienie o wykryciu wzorca. |
| 28. | Określanie wzorców wykonywanych poleceń dla SSH i RDP powinno odbywać się na poziomie tworzenia grup użytkowników, dla których tworzony jest dostęp lub na poziomie grupy systemów docelowych do których dostęp jest chroniony i monitorowany przez rozwiązanie PAM. |
| 29. | Możliwość podglądu nagranych sesji video oraz metadanych z poziomu Systemu bez konieczność używania narzędzi firm trzecich. |
| 30. | Możliwość wygenerowania plików video zapisanych w formacie Systemu odpowiednio dla protokołu RDP do formatu mp4 oraz dla protokołu SSH do formatu ttyrec. |
| 31. | Ochrona haseł wprowadzanych do sesji poprzez wykrycie kursora wejściowego w polach wprowadzania hasła lub w oknie kontrola konta użytkownika UAC (User Account Control). |
| 32. | Uwierzytelnienie użytkownika przez login/hasło, certyfikat X.509, klucz w SSH. |
| 33. | Uwierzytelnianie w oparciu o protokoły: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS+. |
| 34. | Możliwość ustawienia dodatkowego zatwierdzenia dostępu dla połączeń do wybranej grupy serwerów przez wskazaną liczbę użytkowników do tego wskazanych. |
| 35. | Możliwość ustawienia dodatkowe zatwierdzanie dostępu w zależności od czasu logowania, np. nie wymagać zatwierdzania dostępu od Poniedziałku do Piątku, w godzinach 8:00-16:00, a we wszystkich pozostałych dniach i godzinach jej wymagać. |
| 36. | Możliwość współdzielenia hasła użytkownika uprzywilejowanego systemu chronionego z poziomu Systemu bez wysyłania mailem lub innym kanałem komunikacyjnym. |
| 37. | Możliwość zatwierdzania dostępu do chronionego systemu z mechanizmem współdzielenie hasła użytkownika uprzywilejowanego chronionego systemu. |
| 38. | Rozwiązanie musi współpracować z systemami klasy SIEM przynajmniej z wykorzystaniem protokołu syslog. |

Wymagania dotyczące wsparcia technicznego.

|  |  |
| --- | --- |
| 1. | Rozwiązanie musi posiadać Wsparcie Techniczne producenta na okres co najmniej 36 miesięcy, liczony od dnia podpisania protokołu odbioru bez uwag. |
|  | Wsparcie Techniczne powinno być świadczone co najmniej w dni robocze (od poniedziałku do piątku) w godzinach od 8:00 do 19:00 (z wyłączeniem dni ustawowo wolnych od pracy) |
| 2. | Wsparcie producenta powinno być świadczone w języku angielskim lub polskim. |
| 3. | Zgłoszenie problemu technicznego będzie możliwe przez co najmniej dwa kanały komunikacyjne: przez dedykowany numer telefoniczny oraz przez Portal Wsparcia Technicznego dostępny przez przeglądarkę internentową umożliwiający zdalne zgłaszanie i monitorowanie statusu zgłoszenia biletu problemowego. |
| 4. | W ramach udzielonego Wsparcia Technicznego Zamawiający musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną bez ograniczeń, co do liczby zgłoszeń. |
| 5. | Dostęp do Portalu Wsparcia Technicznego musi być udzielony dla co najmniej dwóch kont użytkowników. |
| 6. | Obsługa zgłoszeń musi obejmować co najmniej rozwiązywanie problemów technicznych i konfigurację oprogramowania Systemu. |
| 7. | Reakcja na zgłoszenie problemu technicznego nie może być dłuższa niż 1 dzień roboczy. |
| 8. | Usługa Wsparcia Technicznego musi gwarantować dostęp do aktualnych wersji Systemu oraz poprawek (ang. Hotfix), jak też dokumentacji technicznej - co najmniej instrukcji użytkownika i administratora Systemu. |

Inne wymagania.

|  |  |
| --- | --- |
| 1. | Oferowane produkty będą pochodziły z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej. |
| 2. | Oferowane oprogramowanie musi być oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień dostawy Systemu. |
| 4. | System powinien zapewnić obsługę co najmniej 25 jednoczesnych połączeń pomiędzy oferowanym Systemem a chronionymi systemami. |
| 5. | System musi mieć możliwość ochrony nie mniej niż 25 systemów np. serwerów typu Linux, Windows, aktywnych urządzeń sieciowych jak przełączniki, rutery oraz aplikacje. |
| 6. | System powinien umożliwiać dostęp w tym samym czasie dla co najmniej 25 różnych użytkowników. |
| 7. | Wykonawca przeprowadzi szkolenie z instalacji, parametryzacji i administracji oferowanego rozwiązania – czas trwania szkolenia co najmniej 2 x 6 h dla co najmniej 8 osób w siedzibie Zamawiającego. Zamawiający zapewni salę z rzutnikiem multimedialnym. |