System do kontroli, monitoringu i zarządzania dostępem uprzywilejowanym

SPECYFIKACJA TECHNICZNA

Wymagania minimalne oferowanego systemu

część 1 – Pakiet STANDARD

1. Rozwiązania działające 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 platformy chmurowe Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, platformy wirtualne Kernel-based Virtual Machine (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere oraz platformę sprzętową.
4. Rozwiązanie powinno być dostarczone jako jednolity System. Bez potrzeby instalacji na wskazanym systemie operacyjnym. Cały System powinien być wspierany przez dostawcę, to jest zarówno warstwa systemu operacyjnego, jak i aplikacji.
5. Rozwiązanie powinno wspierać natywnie połączenia dla protokołów SSH i RDP do PROXY, oraz SSH/TELNET/RLOGIN/RDP/VNC od PROXY do systemów chronionych.
6. 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.
7. Dla niestandardowych protokołów i wywołania ich klienta, rozwiązanie powinno wspierać technologie dla Microsoft RemoteApp.
8. Możliwość przydzielania uprawnień administracyjnych, dostępowych dla użytkowników na podstawie profili ustawień.
9. 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.
10. 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.
11. Rozwiązanie powinno pozwalać na określenie polityki dostępu przez przypisanie wybranej grupy użytkowników do wskazanej grupy systemów docelowych.
12. 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).
13. Monitorowanie połączeń w czasie rzeczywistym, w tym możliwość podglądu sesji w czasie rzeczywistym z możliwością jej natychmiastowego zakończenia.
14. Zarządzanie zbiorami reguł (polityką) haseł lokalnych użytkowników i administratorów.
15. Możliwość włączenia/wyłączenia rejestrowania sesji dla wybranych grup użytkowników.
16. Możliwość ustawienia dostępu przez portal internetowy, przeglądarkę, co najmniej dla sesji SSH i RDP, bez potrzeby instalacji dedykowanej wtyczki w przeglądarce.

17. 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.
18. Możliwość definiowania systemów docelowych przez określenie adresu IP, nazwy DNS lub możliwość określania przez adres IP sieci i maski.
19. 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.
20. Dla sesji RDP możliwość blokowania połączeń TCP wychodzących na stacji docelowej, serwera Microsoft Windows.
21. Dla sesji RDP możliwość blokowania wybranych procesów na stacji docelowej, serwer Microsoft Windows.
22. 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.
23. Określanie wzorców wykonywanych poleceń dla SSH i RDP powinno odbywać się na poziomie tworzenia grup użytkowników, dla których kreowany jest dostęp lub na poziomie grupy systemów docelowych, do których dostęp jest chroniony i monitorowany przez rozwiązanie PAM.
24. Wsparcie funkcjonalności współdzielenia co najmniej sesji RDP nawiązanej przez użytkownika Systemu z Audytorem, rozumianej jako pełna interakcja - wprowadzanie znaków z klawiatury oraz ruchów myszką.
25. Rozwiązanie powinno umożliwiać uwierzytelnienie użytkownika Systemu certyfikatem oraz użycie tego samego certyfikatu przy logowaniu do docelowego systemu.
26. Ochrona haseł wprowadzanych do sesji poprzez wykrycie kursora wejściowego w polach wprowadzania hasła lub w oknie kontrola konta użytkownika UAC (User Account Control).
27. Uwierzytelnienie użytkownika przez login/hasło, certyfikat X.509, klucz w SSH.
28. Wsparcie dla protokołów, uwierzytelniania: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS+.
29. Możliwość ustawienia dodatkowego zatwierdzenia dostępu dla połączeń do wybranej grupy serwerów przez wskazaną liczbę użytkowników do tego wskazanych.
30. Możliwość ustawienia dodatkowego zatwierdzania 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.
31. Możliwość automatycznego wyszukiwania nowych urządzeń w sieci oraz dodawania jako nowych obiektów chronionych w systemie PAM.
32. Możliwość udostępniania w czasie rzeczywistym statystyk oraz kluczowych wskaźników wydajności.
33. Możliwość tworzenia własnych powiadomień mailowych wysyłanych przez system PAM.
34. Wsparcie tworzenia skryptów logowania dla protokołów połączeniowych Telnet / RLOGIN.
35. Rozwiązanie powinno wspierać natywnie nagrywanie połączenia przy zastosowaniu protokołu WinSCP.
36. Wsparcie integracji systemu PAM z rozwiązaniami klasy SIEM wraz z możliwością filtrowania zdarzeń, które mają być wysyłane do systemu SIEM.
37. Możliwość zarządzania polityką retencji danych gromadzonych przez system PAM.

38. System powinien wspierać agregację połączeń sieciowych.
39. System powinien udostępniać informacje o pakiecie, opcjach oraz metryce posiadanej licencji.
40. System musi wspierać klucze ECDSA dla hostów SSH.
41. Rozwiązanie powinno wspierać tryb konfiguracji klustra wysokiej dostępności (ang. HA – Hight Availability), w którym będą co najwyżej dwa węzły zainstalowanego Systemu.

Wymagania minimalne oferowanego systemu

część 2 – Pakiet PREMIUM

1. Możliwość automatycznego rotowania haseł i kluczy SSH dla określonych hostów lub grup kont.
2. Możliwość tworzenia wyjątków dla automatycznego rotowania haseł i kluczy SSH.
3. Tworzenie różnych harmonogramów automatycznej zmiany haseł na systemach docelowych.
4. Generować hasła jednorazowe oraz zmieniać je automatycznie po ich użyciu.
5. Możliwość tworzenie własnych polityk / wymagań dla haseł:
    a. Wymagalność minimalnej ilości znaków,
    b. Wykluczenie określonych przez administratora znaków,
    c. Wymagalność wielkich i małych liter,
    d. Wymagalność znaków specjalnych,
    e. Wymagalność minimalnej liczby znaków specjalnych.
6. Wymagalność ustawienia różnych polityk/wymagań haseł dla różnych grup hostów lub grup kont.
7. Ustawienie ważności hasła w określonym przedziale czasu.
8. Kontrola haseł znajdujących się w plikach poprzez ich ukrycie lub dekodowanie.
9. Zapewnienie wtyczek pozwalających na zmianę haseł dla systemów: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Micorsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana.
10. Rozwiązanie musi umożliwiać zmianę haseł za pośrednictwem interfejsu API (co najmniej REST API/SCIM API).
11. Zarządzanie oraz cykliczne rotowanie haseł kont serwisowych.
12. Możliwość integracji Systemu z rozwiązaniami AV/DLP przez zastosowanie protokołu ICAP.
13. Dla protokołów WinSCP oraz SFTP wparcie analizowania zawartości przesyłanych plików oraz ich blokowania.
14. Możliwość integracji Systemu z systemami klasy ITSM (ang. IT Service Management).

Wymagania minimalne oferowanego systemu

część 3 – Opcje dodatkowe

część 3.1 – Access Manager

1. Dodatkowo do systemu powinno być rozwiązanie, portal web, który realizuje zarządzenie połączeniami dla protokołów co najmniej SSH i RDP w ramach przeglądarki internetowej.
2. Działanie systemu, realizacja połączeń, powinna być realizowana z wykorzystaniem jedynie przeglądarki internetowej wspierającej HTML5, bez potrzeby instalacji wtyczek (np. flash, java).

3. Wspierana przeglądarki internetowe: Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox.
4. Rozwiązanie powinno być dostarczone jako aplikacja instalowana na jednym z systemów: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Entreprise Linux, CentOS 6.6, Red Hat Entreprise Linux, CentOS 7.1, Debian 8 (amd64).
5. Rozwiązanie powinno realizować funkcję przeszukiwania tzw. global search meta-danych zarejestrowanych sesji dla jednej lub więcej instancji rozwiązania PSM.
6. Wsparcie dla protokołów, uwierzytelniania: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, SAML.
7. Licencja na rozwiązanie musi umożliwiać dostęp dla **3** użytkowników.
8. Licencja na rozwiązanie musi umożliwiać instalacje wielu instancji portalu, tak by np. można wykorzystać jedną instancję na cele dostępowe (PSM), a kolejną dla celów audytowych (wyszukiwanie meta-danych).

część 3.2 – Application-to-Application Password Manager

1. Wsparcie dostępu do haseł lub kluczy SSH przechowywanych w sejfie haseł Systemu bez konieczności interakcji użytkownika.
2. Wsparcie uwierzytelnienia użytkownika za pomocą hasła lub certyfikatu X.509.
3. Wsparcie Systemów Operacyjnych takich jak AIX, Linux oraz Windows.
4. Wsparcie komunikacji z Systemem za pomocą REST API.

część 3.3 – Universal Tunneling

1. System ma umożliwiać wsparcie i ochronę systemów OT

część 3.4 – BestSafe

1. Instalacja systemu powinna być możliwa w istniejącej infrastrukturze Acive Directory, bez konieczność posiadania dodatkowych elementów, jak System Operacyjny i Baza Danych.
2. System powienien umożliwiać elewację uprawnień użytkownika dla zdefiniowanych procesów bez konieczności zmiany kontekstu użytkownika.
3. System powinien umożliwiać tworzenie list Białej / Szarej / Czarnej, które będą dawały możliwość granularnego zarządzania procesami na systemach docelowych.
4. Zarządzanie uprawnieniami dla procesów powinno mieć wsparcie dla systemów:
    a. Microsoft Windows: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Serwer 2003 oraz Windows Serwer 2003 R2, Windows Serwer 2008 oraz Windows Serwer 2008 R2, Windows Serwer 2012 oraz Windows Serwer 2012 R2, Windows Serwer 2016, Windows Serwer 2019
    b. Linux: Debian 10 (Buster), Ubuntu 20.04 LTS, RedHat 7.0, CentOS 7.0, Suse 12.3

5. System musi gwarantować ciągłość wykonywania reguł dla procesów w przypadku braku połączenia urządzeń typu Microsoft Windows oraz Linux z siecią korporacyjną.
6. System powinien zapobiegać manipulowaniu, zmienianiu, odinstalowywaniu lub usuwaniu plików binarnych przez standardowych lub administracyjnych użytkowników.
7. Możliwość wykonywania kwarantanny dla wybranych aplikacji.
8. Możliwosc przypisywania reguł bezpieczeństwa do pojedyńczego elementu lub kontenera AD.

9. Możliwość definiowania reguł bezpieczeństwa z poziomu konsoli administracyjnej udostępnianej w formie MMC (ang. MMC – Microsoft Managment Console).

część 3.5 – Authenticator

1. Rozwiązanie powinno być dostępne w modelu usługowych, gdzie nie ma konieczności instalowania w środowisku klienckim dedykowanego Systemu Operacyjnego oraz Bazy Danych.
2. Zarządzanie rozwiązaniem powinno odbywać się przez konsolę webową (ang. GUI – Grafical User Interface).
3. W panelu administracyjnym powinna być informacja o parametrach takich jak: użytkownicy, zestawione sesje, alarmy systemowe, udostępnione aplikacje, źródła zewnętrzne użytkowników.
4. Możliwość integracji aplikacji z Systemem w oparciu o metody RADIUS lub SAML2.
5. Możliwość zdefiniowania uwierzytelnienia drugim składnikiem, którym będzie SMS, TOTP Authenticator (np. Google Authenticator, Free OTP, Microsoft Authenticator), Trustelem Authenticator – natywny autentykator, klucze bezpieczeństwa oraz certyfikaty.

część 3.6 – HA 3+ węzły

1. Rozwiązanie powinno wspierać tryb konfiguracji klustra wysokiej dostępności (ang. HA – Hight Availability), w którym będą co najmniej trzy węzły zainstalowanego Systemu.

Wymagania minimalne oferowanego systemu

część 4 – WSPARCIE TECHNICZNE

1. Rozwiązanie musi posiadać Wsparcie Techniczne producenta na okres co najmniej 12 miesięcy.
2. 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 wolnych ustawowo od pracy).
3. Wsparcie producenta powinno być świadczone w języku angielskim.
4. Zgłoszenie problemu technicznego będzie możliwe przez conajmniej 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.
5. W ramach udzielonego Wsparcia Technicznego Zamawiający musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną bez ograniczeń co do liczby zgłoszeń.
6. Dostęp do Portalu Wsparcia Technicznego musi być udzielony dla co najmniej **2** kont użytkowników.
7. Obsługa zgłoszeń musi obejmować co najmniej rozwiązywanie problemów technicznych i konfigurację oprogramowania Systemu.
8. Reakacja na zgłoszenie problemu technicznego nie może być dłuższa niż **1** dzień roboczy.
9. 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.

Wymagania minimalne oferowanego systemu

część 5 – LICENCJA

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.
3. System musi mieć możliwość ochrony nie mniej niż 21 systemów np. serwerów typu Linux, Windows, aktywnych urządzeń sieciowych, jak przełączniki, rutery oraz aplikacje np. konsole do zarządzania.
4. System powinien mieć możliwość dostęp do Systemu w tym samym czasie dla co najmniej 3 użytkowników.
5. Oferowana licencja musi zawierać Wsparcie Techniczne zgodne z wymaganiami w części 4 – WSPARCIE TECHNICZNE.