ТЕНДЕРНА ДОКУМЕНТАЦІЯ

Банк оголошує тендер з придбання ліцензій на ПЗ управління доступом і контролю за привілейованими обліковими записами.

Вимоги замовника до програмної продукції
Автоматизована система (АС) являє собою сукупність інформаційних ресурсів (активів) та інформаційних систем (активів, згрупованих на основі завдань, що ними вирішуються), об'єднаних локальними обчислювальними мережами об'єктів Замовника і системами телекомунікацій між об'єктами, з наданням різних прав доступу до інформаційних ресурсів для різних груп користувачів. Кількість привілейованих користувачів автоматизованої системи контролю дій системних адміністраторів: 20 шт. Кількість інформаційних ресурсів для ізоляції, контролю і запису сесій доступу адміністраторів: 400 шт. Кількість інформаційних ресурсів для управління паролями і SSH ключами: 400 шт.
Вимоги замовника до послуг з інсталяції та налаштування
Комерційна пропозиція повинна включати пункт з ціною на послуги на інсталяцію та налаштування ПЗ, згідно якому, постачальник повинен виконати інсталяцію та налаштування програмного забезпечення, відповідно до вимог Замовника. Роботи по інсталяції та налаштування програмного забезпечення повинні виконуватися кваліфікованим інженером.

Вимоги до ПЗ:

Функціональні вимоги до АС
1. Адміністрування об'єктів інфраструктури за протоколом SSH 2. Адміністрування об'єктів інфраструктури за протоколом RDP 3. Адміністрування об'єктів інфраструктури, що мають Web інтерфейс керування (адміністрування за протоколом HTTP / HTTPS) 4. Адміністрування за іншими протоколами. Наявність можливості конфігурації АС для забезпечення безпечного адміністрування об'єктів інфраструктури незалежно від типу протоколу, оцінюється позитивно. 5. Відсутність необхідності встановлення агентів на об'єкти адміністрування для реалізації парольної політики та записи привілейованих сесій. 6. Адміністрування серверів з сімейства ОС UNIX (AIX, HP-UX, Solaris) 7. Адміністрування серверів з сімейства ОС Windows Server (2003, 2008, 2012) 8. Адміністрування контролерів домену Microsoft Windows 9. Адміністрування об'єктів інфраструктури VMware (всіх компонентів) і Microsoft Hyper-V 10. Адміністрування термінальних серверів Citrix 11. Адміністрування серверів СУБД 12. Адміністрування MQ server 13. Адміністрування файлових ресурсів (сервери і NAS) 14. Адміністрування активних комутаторів локальної обчислювальної мережі (далі – ЛОМ) (провідних виробників) 15. Адміністрування активних маршрутизаторів ЛОМ (провідних виробників) 16. Адміністрування міжмережевих екранів (провідних виробників) 17. Адміністрування FC-комутаторів і SAN маршрутизаторів 18. Адміністрування робочих станцій під управлінням ОС сімейства Windows (XP, 7, 8, 10) 19. Забезпечення можливості інтеграції інтерфейсу адміністрування: vsphere client, toad, dbeaver, SQL+, BarracudaNG admin. 20. Архітектура системи повинна передбачати її установку як в «фізичний розрив» (на мережевому рівні) між робочою станцією контрольованих адміністраторів (далі – КА), з якої виконується адміністрування, і об'єктом адміністрування, так і в «логічний розрив», коли без зміни мережевої інфраструктури забезпечується аналогічний функціонал ізоляції сесії адміністрування і неможливість отримання адміністративного доступу до об'єкта адміністрування. 21. Доступ КА до об'єктів адміністрування повинен проводитися через портал адміністрування, на якому КА автентифікується і обирає об'єкт адміністрування з доступних йому відповідно до його функціональних обов'язків. 22. Доступ і зберігання параметрів привілейованих облікових записів, організація відеоархіву операцій

адміністрування об'єктів інфраструктури повинні бути реалізовані на базі захищеного виділеного сховища.

23. Захист сховища повинен забезпечуватися шляхом обмеження доступу до нього за дискреційною моделлю доступу з можливістю використання рольової моделі. Дані в сховищі повинні бути зашифровані. Сховище повинне бути захищене від несанкціонованого доступу.
24. Можливість передачі даних журналів аудиту в систему класу SIEM McAfee.
25. Інтеграція з системами обробки заявок.
26. Інтеграція зі сканером безпеки Rapid7. Повинна бути можливість зберігання параметрів облікового запису, з під якої виконується сканування, в захищеному сховищі АС.
27. Необхідна можливість автоматизації виявлення і імпорту з Microsoft Active Directory об'єктів адміністрування з подальшою автоматичною зміною паролів адміністративних облікових записів на даних об'єктах управління.
28. Процес реєстрації дій КА повинен забезпечувати ізоляцію середовища виконання утиліт адміністрування від потенційно недовіреного середовища робочої станції адміністратора і повну реєстрацію всієї відеоінформації, що спостерігається адміністратором на своїй консолі.
29. Можливість підключення до сесії адміністрування в режимі "View Only"
30. Кількістю одночасних сесій адміністрування має становити не менше 100 з'єднань.
31. Система повинна мати єдину консоль управління всіма функціональними модулями системи.
32. Система повинна мати можливість зберігання привілейованих облікових записів, та надавати їх адміністратору в сесію без розкриття
33. АС повинна вести свій власний журнал аудиту дій всіх працюючих через неї облікових записів.
34. У журналах аудиту АС відображається інформація про ідентифікаційні і автентифікаційні параметри КА (проводиться однозначне зіставлення адміністратора і використовуваного облікового запису).
35. У журналах аудиту АС відображається інформація про всі дії КА.
36. У журналах аудиту АС відображаються команди КА при використанні текстових протоколів.
37. Відсутність можливості знищення журналів аудиту під обліковим записом будь-якого КА системи.
38. У журналах аудиту АС відображається інформація про параметри відеозаписів сесій КА.
39. Повнотекстовий пошук по журналах аудиту об'єктів адміністрування, відновлення часової послідовності подій, що відбувалися в рамках сесій адміністрування конкретного КА з доступними об'єктами адміністрування.
40. Забезпечення пошуку по відеоархіву (дата, час, користувач, об'єкти адміністрування).
41. Забезпечення пошуку за командами в незавершених сесіях.
42. Можливість вивантаження відеозаписів для подальшого перегляду.
43. Забезпечення захисту від модифікацій і маніпуляцій із записаними сесіями.
44. Неможливість видалення із захищеного сховища будь-якого файлу від імені будь-якого користувача в межах 90 денного терміну (параметр налаштовується).
45. Формування статистичних звітів без необхідності залучення зовнішніх генераторів звітів або вивантаження інформації в зовнішні системи.
46. Забезпечення можливості виявлення фактів і спроб підключення до об'єктів управління в обхід створюваної АС.
47. Автоматичний аналіз дій адміністраторів на основі накопичуваної в АС статистичної інформації та попередження відповідальних осіб про виявлення відхилення поведінки адміністратора від статистичної норми.
48. Двостороння інтеграція модуля поведінкового аналізу з SIEM системою: прийом інформації з SIEM і повернення результатів аналізу в SIEM
49. АС повинна підтримувати реалізацію у вигляді високодоступного георосповсюдженого кластера з можливістю перемикання між вузлами без втрати інформації.
50. Можливість централізованого управління територіально розподіленими компонентами АС
51. Діагностичні засоби АС повинні дозволяти виконувати завдання з моніторингу роботи АС. У разі використання стандартного комплексу технічних засобів, моніторинг може виконувати зовнішніми системами, наприклад Microsoft operation manager.
52. При використанні власної програмно-апаратної платформи моніторинг повинен забезпечуватися власним ПО, або повинна підтримуватися інтеграція із стандартними засобами.

Наявність процедури аварійного відновлення параметрів облікових записів в разі виходу з ладу модулів АС.

Вимоги інформаційної безпеки

1. Забезпечення режиму аутентифікації за логіном / паролем
2. Забезпечення режиму аутентифікації на основі протоколу RADIUS
3. Забезпечення режиму аутентифікації на основі протоколу SAML 2.0
4. Забезпечення режиму аутентифікації на основі протоколу LDAP
5. Наявність можливості визначення переліку IP-адрес, з яких дозволяється доступ до об'єктів інфраструктури для їх адміністрування.
6. АС повинна дозволяти створювати рольову модель її адміністрування.

7. Всі глобальні налаштування повинні виконуватися з-під облікового запису головного адміністратора, використання якого в штатній роботі АС не потрібно.
8. Налаштування ролі «Контрольований адміністратор». Основна функціональна роль в АС, що дозволяє виконувати адміністраторам об'єктів інфраструктури свої безпосередні функціональні обов'язки за допомогою АС.
9. Налаштування ролі «Офіцер безпеки». Додаткова функціональна роль в АС, яка використовується за необхідністю, що дозволяє погоджувати (підтверджувати / відхиляти) доступ КА до об'єктів інфраструктури.
10. Розмежування доступу до об'єктів ІТ-інфраструктури за ідентифікатором КА
11. Розмежування доступу до елементів ІТ-інфраструктури за тимчасовим діапазоном
12. Розмежування доступу до елементів ІТ-інфраструктури за кількістю підключень (Багаторазовий або одноразовий доступ)
13. Можливість керування дозволом на виконання окремих команд / запуск устаткувань адміністрування в сесії адміністрування серверних систем (Unix і Windows).
14. Можливість формування списку.
15. Забезпечення режиму «чотирьох очей», при якому спостерігач за діями КА уповноважений співробітник має можливість на свій розсуд перервати сесію роботи КА
16. Реалізація процесу узгодження надання доступу до об'єктів управління і реєстрацію фактів наділення доступом
17. Забезпечення відеозапису сесій адміністрування всіх підтримуваних об'єктів інфраструктури, в тому числі об'єктів з нестандартними інтерфейсами адміністрування
18. Наявність можливості створювати часткову резервну копію захищеного сховища, що містить інформацію про параметри привілейованих облікових записів, з під яких ведеться адміністрування об'єктів інфраструктури.
19. Можливість виділення на носій, що не приймається, майстер-ключа, необхідного для надання прав доступу до адміністрованих об'єктів в аварійному режимі.
20. Можливість примусового виборчого закриття сесій адміністрування, здійснюваних через АС
21. Реалізація маскування / демонстрації паролів на обліковий запис КА (реалізація функціоналу демонстрації пароля для одноразової сесії адміністрування).
22. Система повинна підтримувати в якості ключової інформації: паролі і SSH ключі
23. Процес управління привілейованими обліковими записами повинен забезпечувати генерацію нового пароля необхідного рівня складності відповідно до вимог парольної політики, регулярну зміну паролів на об'єктах управління.
24. Система повинна мати як глобальну єдину політику роботи з ключовою інформацією на об'єктах управління, так і можливість створення індивідуальних політик для окремих груп об'єктів управління

Автоматизація повного циклу життя ключової інформації: генерація, призначення на об'єкт управління, періодична перевірка актуальності пральний інформації, зміна за розкладом.