ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованим доступом в інформаційній системі організації»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр СЕЛІТРАРЬ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
СЕЛІТРАРЬ Олександр
(прізвище, ім'я)

Керівник К.т.н., доцент ВЛАСЕНКО Вадим
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СТК
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Селітраря Олександра Олександровича
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія управління привілейованим доступом в інформаційній системі організації»

керівник кваліфікаційної роботи ВЛАСЕНКО Вадим Олександрович
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року №320.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
привілейований доступ;
управління привілейованим доступом;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз поняття привілейованого доступу до інформаційної системи організації.

2. Методи та засоби управління привілейованого доступу інформаційної системи організації.

3. Технологія управління привілейованим доступом до інформаційної системи організації.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності теми роботи.	01.10.2024 р.	
2.	Аналіз поняття захисту привілейованого доступу до інформаційної системи організації.	12.10.2024 р.	
3.	Методи та засоби управління привілейованого доступу до інформаційної системи організації.	27.10.2024 р.	
4.	Технологія управління привілейованим доступом до інформаційної системи організації.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо застосування технологія управління привілейованим доступом до інформаційної системи організації.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Олександр СЕЛІТРАРЬ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Вадим ВЛАСЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача: Селітрарь Олександра

на тему: «Технологія управління привілейованим доступом в інформаційній системі організації».

Актуальність: Питання управління привілейованим доступом (Privileged Access Management, PAM) сьогодні відіграє значну роль для захисту інформаційних систем організацій. Це пов'язано з тим, що кіберзлочинці використовують все більше витончені атаки на інформаційні системи. В інформаціних системах привілейований доступ має доступ до критично важливих систем і всієї інфраструктури організації. Отримання зловмисниками доступ до привілейованого доступу може призвести до великих фінансових збитків і втрати даних. Тому організації повинні відповідати стандартам у сфері захисту інформації, таким як GDPR та ISO 27001, які вимагають від організацій впроваджувати контроль та захищати доступ до інформаційної системи організації. Тому тема кваліфікаційної роботи є актуальною і своєчасною.

Позитивні сторони:

1. Проведено дослідження поняття управління привілейованим доступом до інформаційної системи організації.
2. Достатньо успішно викладено матеріали щодо архітектури та компонентів технології Arcon PAM.
3. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. В роботі доцільно було б продемонструвати роботу технології Arcon PAM для заданої величини організації.
2. В роботі не висвітлено інші моделі доступу, за якими можна організувати привілейований доступ.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач **СЕЛІТРАРЬ Олександр** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ та ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач **СЕЛІТРАРЬ Олександр** до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія управління привілейованим доступом в інформаційній системі організації»

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач **СЕЛІТРАРЬ Олександр** обрав тему роботи, метою якої було дослідити технологію управління привілейованим доступом до інформаційної системи організації. Під час виконання кваліфікаційної роботи **СЕЛІТРАРЬ Олександр** показав гарну теоретичну та практичну підготовку, вміння вирішувати самостійно питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **СЕЛІТРАРЯ Олександра** на оцінку **«добре»** та присвоїти йому кваліфікацію: магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Вадим ВЛАСЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СЕЛІТРАРЬ Олександр** допускається до захисту даної кваліфікаційної роботи в екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 62 сторінки, 16 рисунка, 1 таблиця, 11 джерел.

Об'єкт дослідження – управління привілейованим доступом до інформаційної системи організації.

Предмет дослідження – технологія управління привілейованим доступом до інформаційної системи організаціїна прикладі Arcon PAM .

Метою роботи – роботи розробка варіанту технології управління привілейованим доступом в інформаційній системі організації та розробка рекомендації щодо її застосування.

Методи дослідження – вивчення літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

В роботі проведено аналіз поняття привілейоваого доступу до інформаційної системи організації. В результаті аналізу визначено важливість застосування технології управління привілейованим доступом, яка може захистити від несанкціонованого доступу до інформаційної системи організації та інших атак, які можуть призвести до витоку конфіденційної інформації. В роботі досліджено методи та засоби управляння привілейованим доступом на прикладі рішення Arcon PAM. Запропонована технологія дозволяє працювати привілейованими обліковими записам, створювати та зберігати паролі, моніторити сеанси привілейованих користувачів. В роботі запропоновано варіант технології привілейованого доступу. Надано рекомендації щодо роботи інформаційної панелі Arcon PAM та організації зміни паролів користувачів.

Галузь застосування - кібербезпека інформаційних систем організацій.

ІНФРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ПРИВІЛЕЙОВАНИЙ ДОСТУП, ОБЛІКОВИЙ ЗАПИС, УПРАВЛІННЯ, КОРИСТУВАЧІ, ПАРОЛЬ, СЕЙФ, МОНІТОРИНГ, СЕАНСИ, ТЕХНОЛОГІЯ

ABSTRACT

The text part of the qualification work: 62 pages, 16 figures, 1 table, 11 sources..

Object of research – management of privileged access to an organization's information system.

Subject of research – technology of managing privileged access to organization's information system using Arcon PAM.

The aim of research – work on the development of a variant of privileged access management technology in the organization's information system and the development of a recommendation for its application..

Research methods –the studying the literature on this topic, analysing operational documentation, international standards and comparing them.

The paper analyzes the concept of privileged access to the organization's information system. As a result of the analysis, the importance of the use of privileged access management technology, which can protect against unauthorized access to the organization's information system and other attacks that can lead to the leakage of confidential information, is determined. The work examines the methods and means of managing privileged access using the Arcon PAM solution as an example. The proposed technology allows working with privileged accounts, creating and saving passwords, monitoring sessions of privileged users. The work offers a variant of the privileged access technology. Recommendations are provided for the operation of the Arcon PAM dashboard and the organization of changing user passwords.

Field of application – cybersecurity of enterprise information systems.

INFORMATION SYSTEM, CYBERSECURITY, PRIVILEGED ACCESS, ACCOUNT, MANAGEMENT, USERS, PASSWORD, SAFE, MONITORING, SESSIONS, TECHNOLOGY

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CIEM– Cloud infrastructure entitlement management

IAM – Identity and Access Management

PAM – Privileged Access Manager

PASM – Privileged account and session management

PEDM – Privilege elevation and delegation management

PIM – Privileged Identity Management

PSM – Privileged Session Manager

PTA – Privileged Threat Analytics

SIEM – Security Information and Event Management

VPAM – Vendor privileged access management

SSO – Single Sign-On

ВСТУП

У сучасному цифровому світі інформація стала одним із найцінніших активів будь-якої організації. Відповідно, захист цієї інформації від несанкціонованого доступу є одним із найважливіших завдань. Особливу загрозу становитимуть внутрішні загрози, пов'язані з діями привілейованих користувачів, які мають широкі права доступу до інформаційних систем.

Привілейовані користувачі, такі як адміністратори систем, мають широкий спектр дозволів, що дозволяє їм виконувати різноманітні дії в системі. З одного боку, це необхідно для забезпечення нормального функціонування системи, з іншого – створює значні ризики. Якщо облікові записи привілейованих користувачів будуть скомпрометовані, зловмисники зможуть отримати повний контроль над системою, викрасти конфіденційні дані, вивести систему з ладу або навіть використовувати її для атак на інші системи.

Для вирішення проблеми управління привілейованим доступом розробляються різноманітні технології та рішення. Одним із найефективніших методів є використання спеціалізованих систем управління привілейованим доступом (Privileged Access Management, PAM). Такі системи дозволяють централізовано керувати обліковими записами привілейованих користувачів, контролювати їхню активність, а також забезпечувати додаткові механізми захисту, такі як розподіл обов'язків між різними користувачами для зменшення ризику зловмисних дій одного користувача, надання тимчасового доступу до ресурсів лише тоді, коли це необхідно для виконання конкретної задачі, реєстрація всіх дій привілейованих користувачів для подальшого аналізу та виявлення підозрілої активності, регулярна зміна паролів для ускладнення підбору паролів зловмисниками, використання додаткових факторів аутентифікації (наприклад, SMS-коди, одноразові паролі) для підвищення рівня захисту.

Ефективне управління привілейованим доступом неможливе без дотримання чисельних нормативних документів, таких як GDPR, PCI DSS, HIPAA та ін. Ці

документи встановлюють вимоги щодо захисту персональних даних, інформації про платіжні картки, даних у сфері охорони здоров'я тощо. Дотримання цих вимог є обов'язковим для багатьох організацій і дозволяє уникнути значних штрафів та репутаційних втрат.

Саме тому проблема управління привілейованим доступом є надзвичайно актуальноюі своєчасною.

Об'єкт дослідження – управління привілейованим доступом до інформаційної системи організації.

Предмет дослідження – технологія управління привілейованим доступом до інформаційної системи організації на прикладі Arcon PAM.

Метою роботи – роботи розробка варіанту технології управління привілейованим доступом в інформаційній системі організації та розробка рекомендації щодо її застосування.

Методи дослідження – вивчення літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Наукові завдання:

дослідити сутність поняття управління привілейованим доступом інформаційної системи організації;

аналіз ризиків управління привілейованими користувачами;

провести аналіз технологій управління привілейованим доступом;

дослідити методи та засоби управління привілейованим доступом до інформаційної системи організації;

розкрити порядок реалізації технології управління привілейованим доступом на прикладі ARCON PAM;

надати рекомендації щодо використання ARCON PAM для управління привілейованим доступом.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління привілейованим доступом CyberArk PAM, а також розроблено рекомендації для фахівців з кібербезпеки щодо застосування даної технології.

Результати роботи доповідались на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки» м. Київ, 25 жовтня 2024 року.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз поняття управління привілейованим доступом інформаційної системи організації

Фахівці з кібербезпеки в своїй професійній діяльності зустрічаються з поняттям управління ідентифікацією та доступом та управління привілейованим доступом.

Управління ідентифікацією та доступом (IAM) — це широке поле, яке охоплює всі зусилля організації щодо безпеки ідентифікації для всіх користувачів і ресурсів. PAM — це підмножина IAM, яка зосереджена на захисті привілейованих облікових записів і користувачів [1].

Між IAM і PAM існує значне збігання. Обидва включають надання цифрової ідентифікації, впровадження політик контролю доступу та розгортання систем автентифікації та авторизації [1].

Однак PAM йде далі, ніж стандартні заходи IAM, оскільки привілейовані облікові записи вимагають більш надійного захисту, ніж стандартні облікові записи. Програми PAM використовують розширені заходи безпеки, такі як сховища облікових даних і запис сеансу, щоб суворо контролювати, як користувачі отримують підвищені привілеї та що вони з ними роблять.

Було б непрактично й неефективно застосовувати такі жорсткі заходи до непривілейованих облікових записів. Ці заходи зупинять звичайний доступ користувачів і ускладнять людям виконання повсякденної роботи. Ця різниця у вимогах безпеки є причиною того, що PAM та IAM розділилися на окремі, але пов’язані дисципліни.

Керування привілейованим доступом (PAM) — це дисципліна кібербезпеки , яка керує та захищає привілейовані облікові записи (наприклад, облікові записи адміністратора) і привілейовану діяльність (наприклад, роботу з конфіденційними даними).

Таблиця 1.1.

Порівняння PAM та IAM

PAM Управління привілейованим доступом	IAM Управління доступом до особистих даних
Зосереджено на управлінні адміністративними та привілейованими користувачами	Зосереджено на автентифікації та авторизації звичайних користувачів
Користувачі матимуть доступ до більшої кількості привілейованих облікових записів і бізнес-технічних функцій	Користувачі матимуть доступ до невеликої кількості бізнес-додатків
Обмежені стандартні протоколи	Велика екосистема протоколів і механізм автентифікації для захисту особистих даних
Покриває меншу поверхню атаки	Охоплює велику поверхню атаки доступу користувачів усієї організації

У комп'ютерній системі «привілеї» стосуються прав доступу, які вищі, ніж у стандартного користувача. Звичайний обліковий запис користувача може мати дозвіл на перегляд записів у базі даних, тоді як привілейований адміністратор зможе налаштовувати, додавати, змінювати та видаляти записи.

Користувачі, які не є людьми, наприклад машини, програми та робочі навантаження, також можуть мати підвищені привілеї. Наприклад,

автоматизований процес резервного копіювання може мати доступ до конфіденційних файлів і налаштувань системи.

Управління привілейованим доступом поєднує процеси та технологічні інструменти, щоб контролювати, як привілеї призначаються, доступ і використовуються. Багато стратегій PAM зосереджені на трьох стовпах [2, 3]:

Керування привілейованими обліковими записами: створення, надання та безпечне видалення облікових записів із підвищеними дозволами.

Керування привілеями: керування тим, як і коли користувачі отримують привілеї, а також те, що користувачі можуть робити зі своїми привілеями.

Керування привілейованим сеансом: моніторинг привілейованої активності для виявлення підозрілої поведінки та забезпечення відповідності.

Основні компоненти керування привілейованим обліковим записом

Керування привілейованими обліковими записами керує всім життєвим циклом цих привілейованих облікових записів, зокрема:

Виявлення: інвентаризація всіх існуючих привілейованих облікових записів у мережі.

Надання: створення нових привілейованих облікових записів і призначення дозволів на основі принципу найменших привілеїв.

Доступ: керування тим, хто та як може отримати доступ до привілейованих облікових записів.

Утилізація: безпечне видалення привілейованих облікових записів, які більше не потрібні.

Основною метою керування привілейованими обліковими записами є зменшення кількості привілейованих облікових записів у системі та обмеження доступу до цих облікових записів. Керування обліковими даними є ключовим інструментом для досягнення цієї мети.

Замість того, щоб призначати привілейовані облікові записи окремим користувачам, багато систем PAM централізують ці облікові записи та зберігають їхні облікові дані в сховищі паролів. У сховищі надійно зберігаються паролі, токени, ключі Secure Shell (SSH) та інші облікові дані в зашифрованому вигляді.

Коли користувачеві — людині чи нелюдині — потрібно виконати привілейовану дію, він повинен перевірити облікові дані відповідного облікового запису зі сховища.

Наприклад, скажімо, член IT-групи повинен внести зміни в ноутбук компанії. Для цього їм потрібно використовувати локальний обліковий запис адміністратора цього ноутбука. Облікові дані для облікового запису зберігаються в сховищі паролів, тому член IT-команди починає із запиту пароля облікового запису.

Щоб підтвердити свою особу , член команди повинен спочатку пройти перевірку надійної автентифікації , наприклад багатофакторну автентифікацію (MFA). Потім сховище використовує контроль доступу на основі ролей (RBAC) або подібні політики, щоб визначити, чи дозволено цьому користувачеві доступ до облікових даних для цього облікового запису.

Цьому члену IT-групи дозволено використовувати цей обліковий запис локального адміністратора, тому сховище облікових даних надає доступ. Член IT-групи тепер може використовувати обліковий запис локального адміністратора, щоб вносити необхідні зміни в ноутбук компанії.

Для додаткової безпеки багато сховищ облікових даних не надають облікові дані безпосередньо користувачам. Натомість вони використовують систему єдиного входу (SSO) і посередництво сеансів, щоб ініціювати безпечні з’єднання, при цьому користувач ніколи не бачить пароль.

Термін доступу до облікового запису користувача зазвичай закінчується через установлений проміжок часу або після виконання завдання. Багато сховищ облікових даних можуть автоматично змінювати облікові дані за розкладом або після кожного використання, що ускладнює зловмисникам викрадення та неправильне використання цих облікових даних.

В організації існує кілька типів привілейованих облікових записів. До них належать [4]:

1. Адміністративні облікові записи: повний доступ до системи, включаючи встановлення програмного забезпечення та керування користувачами.

2. Кореневі облікові записи: у середовищах Linux або Unix облікові записи root мають необмежений доступ до всіх команд і файлів.

3. Облікові записи служб: використовуються програмами для взаємодії з операційною системою або іншими програмами.

4. Облікові записи привілейованих користувачів: Особисті облікові записи користувачів із підвищеними привілеями, ніж стандартні користувачі.

5. Облікові записи третіх сторін: використовуються зовнішніми постачальниками для доступу до системи та виконання завдань.

6. Керування цими обліковими записами має вирішальне значення для захисту критично важливих систем і даних.

1.2. Аналіз загроз привілейованому доступу до інформаційної системи організації

Привілейовані облікові записи є цінними цілями для хакерів, які можуть зловживати своїми правами доступу, щоб викрасти дані та пошкодити критичні системи, уникаючи виявлення. Фактично, викрадення дійсних облікових записів є найпоширенішим вектором кібератак сьогодні, згідно з Індексом аналізу загроз IBM® X-Force® .

Інструменти та методи PAM допомагають організаціям захистити привілейовані облікові записи від атак на основі ідентифікаційних даних. Зокрема, стратегії PAM зміцнюють рівень безпеки організації, зменшуючи кількість привілейованих користувачів і облікових записів, захищаючи привілейовані облікові дані та дотримуючись принципу найменших привілеїв.

Привілейовані облікові записи становлять підвищений ризик безпеки . Їхні підвищені дозволи готові для зловживань, і багатьом організаціям важко відстежувати привілейовану активність у локальних і хмарних системах. PAM допомагає організаціям отримати більше контролю над привілейованими обліковими записами, щоб зупинити хакерів , одночасно підключаючи користувачів із потрібними дозволами.

Атаки на основі ідентифікації, під час яких хакери захоплюють облікові записи користувачів і зловживають їхніми дійсними привілеями, зростають. IBM X-Force повідомляє , що минулого року ці атаки зросли на 71%. Зараз на них припадає 30% порушень безпеки . Ці атаки часто спрямовані на привілейовані облікові записи, або безпосередньо, або через латеральне переміщення .

Зловмисники — внутрішні загрози чи зовнішні зловмисники — які заволодіють привілейованими обліковими записами, можуть завдати серйозної шкоди. Вони можуть використовувати підвищені дозволи для розповсюдження зловмисного програмного забезпечення та доступу до критично важливих ресурсів без обмежень, обманюючи рішення безпеки, змушуючи їх вважати себе законними користувачами з дійсними обліковими записами.

Відповідно до звіту IBM Cost of a Data Breach Report , порушення, у яких хакери використовують викрадені облікові дані, є одними з найдорожчих — у середньому 4,62 мільйона доларів США. Інсайдерські загрози, які зловживають своїми дійсними привілеями, можуть завдати ще більшої шкоди, у середньому ці порушення коштують 4,90 мільйона доларів США.

Крім того, цифрова трансформація та розвиток штучного інтелекту збільшили кількість привілейованих користувачів у середній мережі. Кожна нова хмарна служба, програма AI, робоча станція та пристрій Інтернету речей (IoT) приносять нові привілейовані облікові записи. Ці облікові записи включають як облікові записи адміністратора, необхідні користувачам для керування цими активами, так і облікові записи, які ці активи використовують для взаємодії з мережевою інфраструктурою.

Ще більше ускладнює ситуацію те, що люди часто діляться привілейованими обліковими записами. Наприклад, замість того, щоб призначати кожному системному адміністратору власний обліковий запис, багато IT-команд створюють один обліковий запис адміністратора для кожної системи та надають облікові дані користувачам, яким вони потрібні.

У результаті організаціям важко відстежувати привілейовані облікові записи, у той час як зловмисники зосереджують свою увагу саме на цих облікових записах.

Технології та стратегії PAM допомагають організаціям отримати більше видимості та контролю над привілейованими обліковими записами та діями, не порушуючи законні робочі процеси користувачів. Центр безпеки в Інтернеті перераховує основні дії PAM серед своїх «критичних» заходів безпеки. 1

Такі інструменти, як сховища облікових даних і своєчасне підвищення привілеїв, можуть полегшити безпечний доступ для користувачів, які цього потребують, утримуючи при цьому хакерів і неавторизованих інсайдерів. Інструменти моніторингу привілейованих сеансів дозволяють організаціям відстежувати все, що кожен користувач робить зі своїми привілеями в мережі, дозволяючи IT-групам і командам безпеки виявляти підозрілу активність.

1.3. Підходи до вирішення проблеми безпеки привілейованого доступу до інформаційної системи організацій

Хоча інструменти та тактики PAM керують привілейованою діяльністю в організації, вони також можуть допомогти у вирішенні певних проблем безпеки ідентифікації та доступу.

Звуження поверхні атаки на ідентифікацію

Управління розповсюдженням ідентичності

Відповідність нормативним вимогам

Керування секретами DevOps

Звуження поверхні атаки на ідентифікацію

Зловмисники все частіше використовують дійсні облікові записи для проникнення в мережі. У той же час багато організацій страждають від розповзання привілеями. Користувачі мають вищі привілеї, ніж їм потрібно, а застарілі привілейовані облікові записи не вилучаються належним чином.

У результаті особисті дані стали найбільшою небезпекою для багатьох організацій. Інструменти та тактики PAM можуть допомогти усунути ці вразливості.

Сховища облікових даних ускладнюють крадіжку привілейованих облікових записів, а інструменти PEDM забезпечують детальний найменш привілейований доступ, який обмежує бічне переміщення. Організації можуть використовувати ці та інші рішення PAM, щоб замінити постійні привілеї моделлю нульової довіри , де користувачі повинні бути автентифіковані та авторизовані для кожного підключення та активності. Ця модель може допомогти зменшити площу атаки на ідентифікацію та обмежити можливості хакерів.

Управління розповсюдженням ідентичності

Цифрова трансформація спричинила вибух привілейованих ідентифікацій у корпоративних мережах, що створює серйозну проблему для інформаційної безпеки.

Середній бізнес-відділ використовує 87 різних додатків SaaS 3 , не кажучи вже про різноманітні пристрої IoT, служби хмарної інфраструктури та віддалених користувачів із пристроями BYOD , які зараз заповнюють корпоративні мережі. Багато з цих активів і користувачів потребують привілейованих облікових записів для взаємодії з IT-ресурсами.

І оскільки все більше організацій впроваджують генеративний штучний інтелект у свою діяльність, ці нові програми та інтеграції штучного інтелекту виводять на сцену ще один набір привілейованих ідентифікацій.

Багато з цих привілейованих ідентифікацій належать користувачам, які не є людьми, наприклад додатки AI та пристрої IoT. Сьогодні в багатьох мережах нелюди перевищують кількість користувачів-людей, і вони, як відомо, погано зберігають свої облікові дані в таємниці. Наприклад, деякі програми скидають свої облікові дані у вигляді звичайного тексту в системні журнали та звіти про помилки.

PAM може допомогти організаціям керувати розповсюдженням ідентичності, зберігаючи привілейовані облікові дані для людей і нелюдей і централізовано контролюючи доступ до них. Автоматизована ротація облікових

даних може обмежити шкоду від витоку облікових даних, а інструменти моніторингу сеансу допомагають відстежувати, що всі ці різні користувачі роблять зі своїми привілеями.

Відповідність нормативним вимогам

Положення про конфіденційність і безпеку даних, такі як Закон про перенесення та підзвітність медичного страхування (HIPAA), Стандарт безпеки даних індустрії платіжних карток (PCI DSS) і Загальний регламент захисту даних (GDPR), вимагають, щоб організації контролювали доступ до медичної інформації, номерів кредитних карток і інші конфіденційні дані.

PAM може допомогти організаціям виконати вимоги відповідності кількома способами. Інструменти PAM можуть надавати детальні привілеї доступу, щоб лише необхідні користувачі могли отримати доступ до конфіденційних даних і лише з дозволених причин.

Сховища облікових даних і підвищення привілеїв усувають потребу в спільних облікових записах адміністратора, що може призвести до доступу неавторизованих користувачів до конфіденційних даних.

Моніторинг привілейованого сеансу допомагає організаціям відносити дії та створювати журнали аудиту, щоб підтвердити відповідність у разі порушення або розслідування.

Керування секретами DevOps

Керування привілейованими обліковими даними, які в середовищах DevOps часто називають «секретами», може бути особливо складним для команд DevOps.

Методологія DevOps активно використовує хмарні сервіси та автоматизовані процеси, тобто існує багато привілейованих людей і нелюдей, розкиданих по різних частинах мережі.

Нерідко ключі SSH, паролі, ключі API та інші секрети жорстко закодовані в додатки або зберігаються як звичайний текст у системах контролю версій та в інших місцях. Це полегшує користувачам отримання облікових даних, коли вони їм потрібні, щоб робочі процеси не порушувалися, але це також полегшує зловмисникам викрадення цих облікових даних.

Інструменти PAM можуть допомогти, зберігаючи секрети DevOps у централізованому сховищі. Лише законні користувачі та робочі навантаження можуть отримати доступ до секретів і лише з законних причин. Сховища можуть автоматично змінювати секрети, щоб викрадені облікові дані швидко ставали марними.

Поширені стратегії керування привілейованим доступом [2, 3]

Нижче наведено стратегії, які допоможуть організаціям забезпечити ефективність впровадження PAM :

Ведіть інвентаризацію всіх привілейованих облікових записів і документуйте будь-які зміни.

Заборонити адміністраторам ділитися обліковими записами.

Обмежте особисті привілейовані облікові записи до одного для кожного адміністратора.

Встановіть і запровадьте політику паролів для паролів.

Змініть усі паролі на всіх пристроях компанії, щоб користувачі не використовували паролі за умовчанням.

Переконайтеся, що паролі привілейованих облікових записів регулярно змінюються, щоб зменшити ризик того, що співробітники, які залишають компанію, можуть скомпрометувати її системи.

Захистіть привілейовані облікові записи за допомогою двофакторної автентифікації.

Обмежити обсяг дозволів для всіх привілейованих облікових записів.

Запровадити розподіл обов’язків між працівниками.

Застосовуйте найменші привілеї, тобто працівникам надаються лише ті привілеї, які їм необхідні для виконання роботи.

Застосовуйте найкращі практики, щоб підвищити рівень користувачів, яким потрібні додаткові права доступу, як-от задокументовані процеси запитів і затвердження.

Використовуйте різні інструменти та методики журналювання та моніторингу, щоб отримати чітке уявлення про дії привілейованих користувачів.

Інформуйте співробітників про зміни в політиках і процедурах привілейованого доступу, щоб переконатися, що вони розуміють, як правильно використовувати та керувати своїми привілейованими обліковими даними.

Документуйте правила та процеси керування обліковим записом і вимагайте перевірки від керівників компанії.

1.4. Аналіз технологій управління привілейованим доступом до інформаційної системи організації

Аналіз технологій для управління привілейованим доступом проводемо на основі дослідження Gartner 2024, яке засновано на відповідних критеріях оцінювання:

1.Здатність до виконання.

Продукт або послуга: оцінює основні продукти, пропоновані постачальником, які конкурують на/обслуговують визначений ринок. Це включає поточні можливості продукту, якість, набори функцій і документацію в кількох категоріях продуктів:

2. Керування життєвим циклом привілейованого облікового запису: функції для керування повним життєвим циклом привілейованих облікових записів, зокрема: створення привілейованих облікових записів і обробка виявлених облікових записів, призначення та керування правами власності та використання, виведення облікового запису з експлуатації, а також можливість перегляду та сертифікації привілейованих облікових записів.

3. Виявлення та адаптація облікових записів: функції виявлення, ідентифікації та підключення привілейованих облікових записів, включаючи можливість підтримувати періодичне, спеціальне або безперервне сканування. Це також включає можливість автоматичного виявлення цільових служб, систем (включно з віртуальними машинами) для подальшого виявлення привілейованих облікових записів, які містяться в них.

4. Управляння привілейованими обліковими даними : функції для керування та захисту визначених системою та підприємством облікових даних привілейованого облікового запису або секретів (включно з ключами SSH). Воно включає створення, зберігання, ротацію та пошук для інтерактивного доступу до цих облікових даних для окремих осіб. Воно також включає ротацію сервісних і програмних облікових записів (тобто вбудованих облікових записів) у цільових системах.

5. Управління привілейованим сеансом: функції для встановлення сеансу, керування, запису та відтворення, моніторингу в реальному часі, фільтрації команд на основі протоколу та розділення сеансів для сеансів привілейованого доступу. Включено функції для керування інтерактивним сеансом за допомогою інструменту PAM, від перевірки облікових даних до реєстрації цих облікових даних, хоча в звичайних випадках облікові дані не розкриваються користувачеві.

6. Привілейований віддалений доступ: функції для безпечних сценаріїв віддаленого привілейованого доступу без VPN, включаючи керування обліковими даними, посередництво сеансів, запис і аудит сеансів, керування життєвим циклом, передавання файлів, MFA, JIT-доступ і застосування принципів найменших привілеїв віддалених привілейованих користувачів. Крім того, він включає додаткові можливості для самообслуговування реєстрації та керування профілями, багатокористувацьку сеансову співпрацю, спонсорство та делеговане адміністрування, федерацію ідентифікації та запити доступу для віддалених привілейованих користувачів.

7. Керування ідентифікацією та секретами робочого навантаження : функції, які дозволяють керувати та посередницьким доступом до облікових даних (таких як паролі, маркери OAuth і ключі SSH) для нелюдських випадків використання, таких як машини, програми, служби, сценарії, процеси та конвеєри DevOps. Він включає в себе можливість генерувати, зберігати, обертати та надавати облікові дані нелюдям (наприклад, через API). Він також включає в себе здатність підтримувати довіру між різними нелюдськими об’єктами з метою обміну секретами, а також керувати авторизаціями та пов’язаними функціями. Він

включає необов’язкову можливість встановити довіру з нелюдською сутністю, не вимагаючи облікових даних, використовуючи інші механізми розпізнавання (включно з аутентифікацією з нульовим фактором). Ідентифікатори IaaS/PaaS також можна використовувати для встановлення довіри зі сховищем. У поєднанні ці функції підтримують управління секретами для динамічних середовищ і роботизованих платформ автоматизації процесів. Це також включає додаткову аналітику для визначення того, чи є облікові записи машини потенційно зловживаними чи вони більше не використовуються, а також керування секретами в інших продуктах керування секретами.

8. Підвищення привілеїв і управління делегуванням UNIX/Linux: функції для забезпечення функцій на основі хоста для застосування політик, щоб дозволити авторизованим командам або програмам працювати з підвищеними привілеями. Ці функції мають виконуватися на фактичній операційній системі (на рівні ядра чи процесу). Рівень підтримки залежить від платформи (UNIX/Linux і macOS). Ця можливість також може забезпечити з’єднання Active Directory (AD), яке застосовує елементи керування AD до систем Linux/UNIX, включаючи можливість автентифікації в цих системах за допомогою облікових даних AD і наскрізних політик GPO. Це також стосується моніторингу цілісності файлів і керування sudo.

9. Підвищення привілеїв і управління делегуванням Windows : функції для забезпечення функцій на основі хоста для застосування політик, щоб дозволити авторизованим командам або програмам працювати з підвищеними привілеями. Адміністратори входитимуть, використовуючи непривілейований обліковий запис, і за потреби підвищуватимуть повноваження. Будь-яка команда, якій потрібен додатковий привілей, повинна проходити через ці інструменти, фактично запобігаючи виконанню небезпечних дій адміністраторами. Ці функції мають виконуватися у фактичній операційній системі (на рівні ядра чи процесу). Рівень підтримки залежить від платформи (Windows).

10. Простота розгортання, обслуговування та суміжної системної інтеграції: це включає в себе функції та функції, які спрощують розгортання рішення PAM, забезпечуючи легкість адміністрування та обслуговування. Це також вимагає

здатності надавати функції та функції для інтеграції та взаємодії з суміжними системами безпеки та керування послугами. Ці системи включають:

Управління ідентифікацією та адміністрування (IGA);

Єдиний вхід (SSO);

Багатофакторна автентифікація (MFA);

Корпоративні каталоги, підтримка гнучких конекторів та інтеграційних платформ;

Загальний доступ до API, інтеграція з системами управління IT-послугами (ITSM);

Системи безпеки та керування подіями (SIEM);

Управління вразливістю.

11. Продуктивність і доступність: це включає в себе функції та функції, які відстежують продуктивність і надають можливості детальної авторизації (наприклад, керування доступом на основі ролей) для інструменту PAM. Він також надає функціональність, яка дозволяє інструменту PAM забезпечувати резервування для цілей аварійного відновлення (DR) або безперервності бізнесу (BC), а також забезпечувати доступність, можливість відновлення та масштабованість. Це обробляється за допомогою архітектури SaaS або за допомогою власних або сторонніх механізмів для балансування навантаження та отримання облікових даних за розбитим склом (якщо інструмент PAM недоступний) у випадку самокерованих інструментів. Ця можливість додатково надає можливість швидко масштабувати продукт відповідно до вимог на вимогу.

12. Управління правами доступу до хмарної інфраструктури (CIEM): Функції для керування ризиками доступу до хмари за допомогою адміністративних засобів керування правами доступу в (багато) хмарних інфраструктурних середовищах (IaaS). Привілейовані права визначають доступ до хмарних ресурсів, привілеї доступу до послуг і дозволи на керування хмарою. Інструменти CIEM використовують аналітику, машинне навчання (ML) та інші методи для виявлення аномалій у правах облікових записів, як-от накопичення привілеїв, а також неактивні та непотрібні дозволи. CIEM дозволяє застосовувати та виправляти

підходи з найменшими привілеями, рекомендуючи та розгортаючи політики. Більшість інструментів CIEM забезпечують інтеграцію з ключовими платформами IaaS, такими як AliCloud, Amazon Web Services (AWS), Google Cloud Platform (GCP) і Microsoft Azure.

13. Загальна життєздатність: включає оцінку загального фінансового стану організації, а також фінансовий і практичний успіх бізнес-одиниці. Також включено ймовірність того, що окремий бізнес-підрозділ буде продовжувати пропонувати та інвестувати в свій продукт PAM, продовжувати пропонувати продукт і продовжувати просувати сучасний рівень у портфоліо продуктів PAM організації. Фактори, які розглядаються, включають загальний фінансовий стан організації на основі загального розміру, її прибутковості та її ліквідності. Життєздатність постачальника на ринку PAM також оцінюється шляхом вивчення ступеня, до якого продажі PAM сприяють загальному доходу, утриманню клієнтів і зростанню доходу від PAM, а також кількості нових клієнтів.

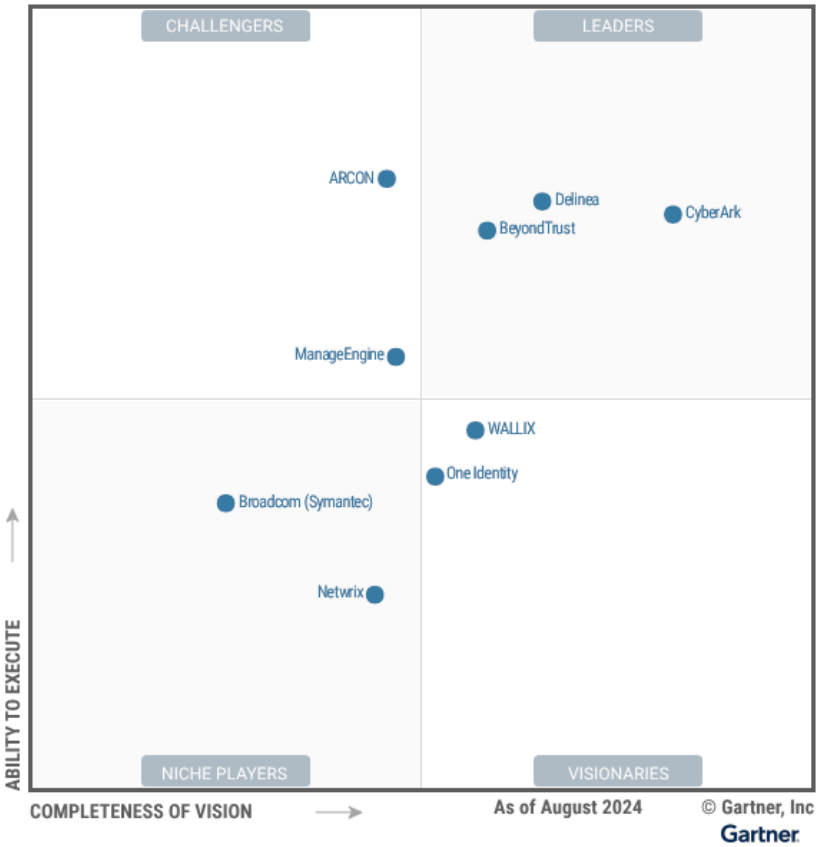

Рис.1.1. Лідери ринку PAM

Arcon

Arcon є претендентом у цьому магічному квадранті. Його пропозиція PAM складається з ARCON PAM Enterprise для привілейованого облікового запису та керування сеансами (PASM) і ARCON EPM для привілейованого підвищення прав і керування делегуванням (PEDM). Обидва доступні як програмне забезпечення та SaaS. ARCON також пропонує кілька додаткових продуктів і модулів , включаючи керування секретами та керування паролями від програми до програми (AAPM), керування віддаленим привілейованим доступом (RPAM), з'єднувачі для інструментів інфраструктури DevOps та керування правами доступу до хмарної інфраструктури (CIEM) . Його операції здебільшого зосереджені в Азіатсько-Тихоокеанському регіоні та регіоні EMEA, хоча постачальник постійно розширює свою базу в пунктах Дорожньої карти США , починаючи з останнього магічного квадранту, що включає вдосконалення доступу до мережі без довіри (ZTNA) для сценаріїв RPAM і покращення операційної ефективності привілейованих дій. через вдосконалення AI.

Сильні сторони

Продукт: пропозиція ARCON є найпотужнішою з усіх оцінених постачальників, причому кожна з можливостей оцінюється вище — а часто й значно вище — середнього рівня . Дві основні функції, за якими Arcon отримує найвищі результати, — це відкриття облікового запису та своєчасне (JIT) PAM ; Arcon продемонструвала значні покращення у випадку використання ефемерних облікових даних JIT.

Ціноутворення : ціни ARCON конкурентоспроможні. У більшості сценаріїв ціноутворення, особливо для PASM, ARCON є доступнішим, ніж пропозиції інших постачальників у цьому дослідженні. У сценаріях PEDM і керування секретами ціна приблизно середня, а іноді й вища за середню , особливо для пропозиції програмного забезпечення .

Взаємодія з клієнтами: ARCON перевершує досвід клієнтів, отримавши один із найвищих балів у цьому дослідженні. Цілодобова підтримка включена для всіх клієнтів, технічний менеджер облікового запису доступний безкоштовно, а також безкоштовна програма навчання продукту.

Загальна життєздатність: зростання кількості клієнтів PAM ARCON за останній фінансовий рік було одним із найвищих серед постачальників, оцінених у цьому дослідженні.

ManageEngine

ManageEngine є претендентом у цьому магічному квадранті. ManageEngine є підрозділом Zoho Corporation, який пропонує низку програмних засобів керування підприємством, у тому числі свій продукт PAM, PAM360. PAM360 пропонує PASM, PEDM, AAPM і деякі функції керування секретами , які об'єднані лише як програмне забезпечення. Він також пропонує Application Control Plus для керування привілеями кінцевих точок і функції контролю програм. ManageEngine наразі не пропонує функції CIEM. Операції ManageEngine є географічно диверсифікованими. Пункти дорожньої карти, починаючи з останнього Magic Quadrant, включають запровадження версії SaaS продукту PAM і можливостей CIEM, а також покращення функціональності привілейованої автоматизації завдань.

Сильні сторони

Ціни: ціни ManageEngine незмінно нижчі за середні ринкові. Він пропонує відмінну модель ціноутворення на основі кількості адміністраторів інструментів PAM (а не кількості привілейованих користувачів , які виконують адміністративні завдання в цільових системах).

Продукт: ManageEngine пропонує потужну функцію PAM « розбити скло » за допомогою підходу до зашифрованого HTML-файлу, який можна зберігати локально або автоматично надсилати до сегментів Dropbox, Box і S3 за допомогою функції офлайн-доступу/хмарної інтеграції.

Дорожня карта вертикальної стратегії: ManageEngine прагне покращити свою підтримку для потреб уряду. У рамках свого плану компанія працює над спеціалізованою версією свого продукту PAM360, яка включатиме елементи керування, розроблені відповідно до унікальних вимог державних клієнтів.

Бізнес-модель : ManageEngine стверджує, що інвестує понад 50% свого доходу в науково-дослідні ініціативи, але має дорожню карту продукту,

розроблену, щоб наздогнати можливості продукту , а також виділитися в інших сферах, таких як керування привілейованим доступом для пристроїв IoT/OT.

WALLIX

WALLIX — провидець у цьому магічному квадранті. Його пропозиція PAM складається з WALLIX Bastion , доступного як програмне забезпечення, і WALLIX One PAM, доступного як SaaS, для функцій PASM і AAPM. Функціональність PEDM надається в WALLIX PAM. Він також пропонує WALLIX One Remote Access, доступний як SaaS, для RPAM. WALLIX не пропонує продукт CIEM, але може надати деякі функції CIEM із суміжним продуктом IGA. Клієнти WALLIX здебільшого знаходяться в регіоні EMEA , деякі з них у Північній Америці, на Близькому Сході та в Африці. Компанія вклала значні кошти, щоб залучити та підтримати клієнтів, які використовують кіберфізичні системи (CPS). Елементи дорожньої карти, починаючи з останнього магічного квадранта, включають централізоване керування приладною дошкою, конфігурацією та адмініструванням для клієнтів, удосконалення керування секретами та нову функціональність для тунелювання в середовищах OT.

Сильні сторони

Продукт: WALLIX отримав одну з найвищих оцінок на ринку за привілейований віддалений доступ і керування сеансами . Для RPAM його WALLIX One Remote Access є одним із найпотужніших на ринку, що пропонує підтримку всіх основних протоколів керування сеансами, включаючи універсальне тунелювання через TCP. Адміністрування ідентифікації, авторизація, сеансова співпраця та можливості передачі файлів для віддалених привілейованих сценаріїв також зрілі.

Вертикальна галузева стратегія: WALLIX виділяється одним із найвищих балів за свою вертикальну стратегію, демонструючи значну присутність у широкому діапазоні галузевих вертикалей (з найкращою у своєму класі підтримкою операційних технологій і галузевих систем управління), а також у виробництві. , банківська справа, цінні папери та страхування та уряд.

Продукт: WALLIX пропонує значущий підхід PAM break - glass, де він може запускати заплановане завдання для періодичної надсилання облікових даних break - glass через зашифровані електронні листи.

Клієнтський досвід: клієнти часто відзначають ефективну та своєчасну підтримку, а також позитивно відгукуються про простоту використання рішення.

Отже, для подальшого дослідження створення технології управління привілейованим доступом будемо використовувати рішення ARCON, яке є найпотужнішою з усіх оцінених постачальників.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ РІШЕННЯ ARCON

2.1. Архітектура платформи платформи ARCON

Рішення ARCON PAM (Privileged Access Management) безпечно управляє, зберігає, архівує та передає всі привілейовані адміністративні паролі всередині інформаційної системи організації як локально, так і віддалено. Всі захищені паролі зберігаються у сховищі паролів.

Сховище паролів, яке виконує функцію «бункера», яке є ядром цього рішення. Воно захищене багатошаровою системою безпеки, що включає брандмауер, автентифікацію, авторизацію, контроль доступу, шифрування, моніторинг сесій тощо. Ці рівні роблять рішення безпечним для привілейованих облікових записів, наявних в організації.

Архітектура PAM дуже проста та легко інтегрується зі складною інфраструктурою підприємства. Її можна розгорнути за короткий період часу, а доступ до неї можна отримати через веб-інтерфейс. Різноманітні API підвищують безпеку рішення.

ARCON PAM має такі основні властивості:

Безпечне масштабування

Безпечне масштабування надає ефективне керування користувачами, підключаючи їх із мережі Microsoft AD, AWS, Azure та GCP, а також дає можливість додавати нові групи серверів, облікові записи користувачів із привілеями до одного екземпляра PAM. Зменшує загрозу втрати привілейованих облікових записів, поширених у неоднорідному IT-середовищі, виявивши всі привілейовані ідентифікатори та пристрої за допомогою автоматичного виявлення.

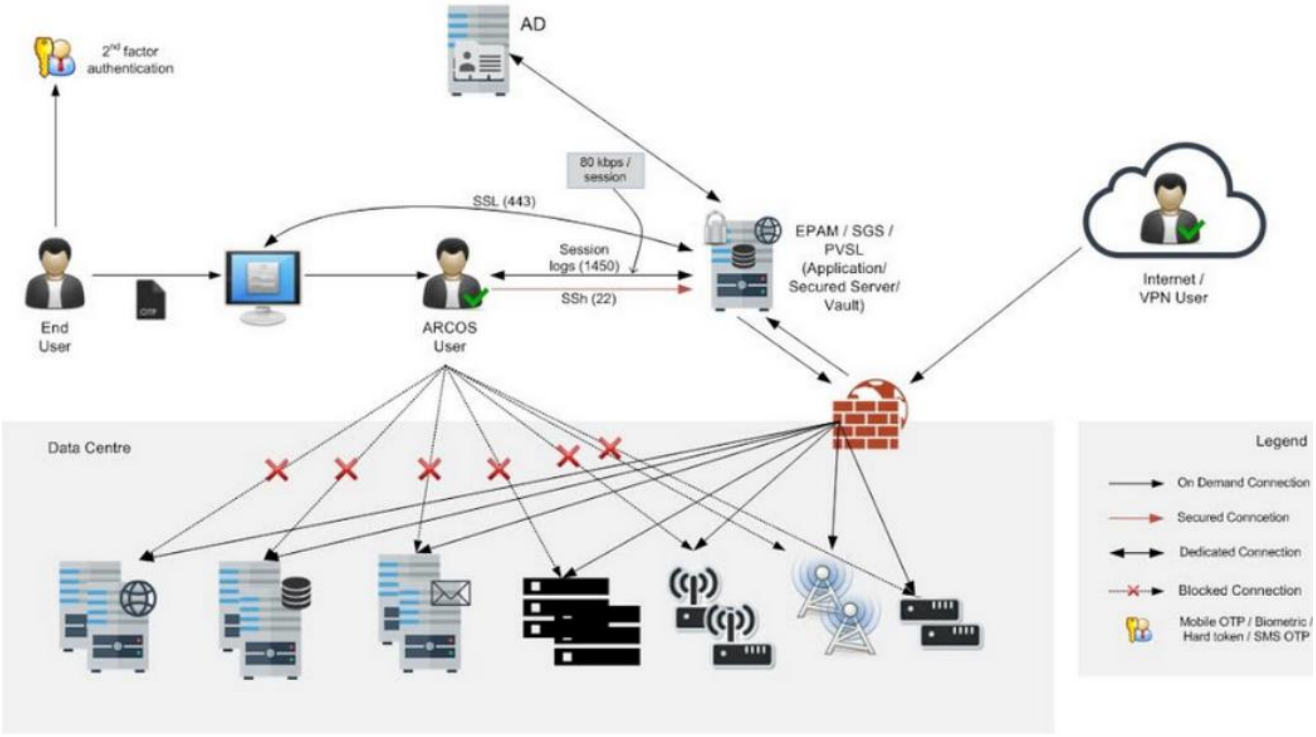

Рис.2.1. Архітектура рішення ARCON PAM

Багатофакторна автентифікація та підходи до нульової довіри

Посилює заходи безпеки та забезпечує дотримання принципів нульової довіри, прийнявши MFA. Окрім вбудованої двофакторної автентифікації, ARCON має повну інтеграцію з усіма сучасними інструментами MFA, такими як автентифікація Google, автентифікація Microsoft, автентифікація ARCON, апаратні маркери, розпізнавання обличчя, біометрична автентифікація, а також традиційні опції, такі як SMS та електронна пошта OTP.

Єдиний вхід та адміністративна ефективність

Співробітникам, яким потрібен одноразовий захищений адміністративний доступ до веб-додатків, застарілих локальних і хмарних додатків, не потрібно турбуватися про керування декількома обліковими даними для доступу до кількох додатків. ARCON SSO підтримує всі стандартні протоколи автентифікації на основі ідентифікації, такі як 0Auth2.0, Open ID Connect (OIDC), Security Assertion Markup Language (SAML).

Контроль доступу та найменші привілеї

Надає доступ на основі «потрібно знати» та «потрібно зробити». Контроль доступу дозволяє керувати привілейованими користувачами на основі їхніх ролей, обов'язків і завдань – дотримуючись принципу найменших привілеїв і знижуючи ризик неавторизованого доступу та неправильного використання конфіденційних систем і даних.

Керування обліковими даними

Застосовує важливі функції та функції для керування та захисту облікових даних/ключів SSH/секретів, призначених для доступу до привілейованих облікових записів. Механізм включає зберігання, рандомізацію та отримання облікових даних для інтерактивного доступу до цільових систем привілейованими користувачами, захищаючи бізнес та інфраструктуру від несанкціонованого доступу.

Керування сеансами

Надаються основні функції для моніторингу, завершення та запису привілейованих сеансів. Забезпечує авторизовані операції в авторизованих системах із виявленням загроз у режимі реального часу та відповідями, а також забезпечує сувору безпеку для надто критичних привілейованих сеансів із тестуванням аудиту для всіх запущених команд і файлів, до яких здійснюється доступ.

Для розуміння функцій всіх копмонентів ARCON PAM представлено місце технології в архітектурі інформаційної системи організації на рис.2.2. Використання технології ARCON PAM з використання показаних компонентів дозволяє впровадити технологію для управління привілейованими ідентифікаційними даними (PIM) / керування привілейованим доступом (PAM), що дозволяє здійснювати моніторинг, керування та аудит привілейованих користувачів [5].

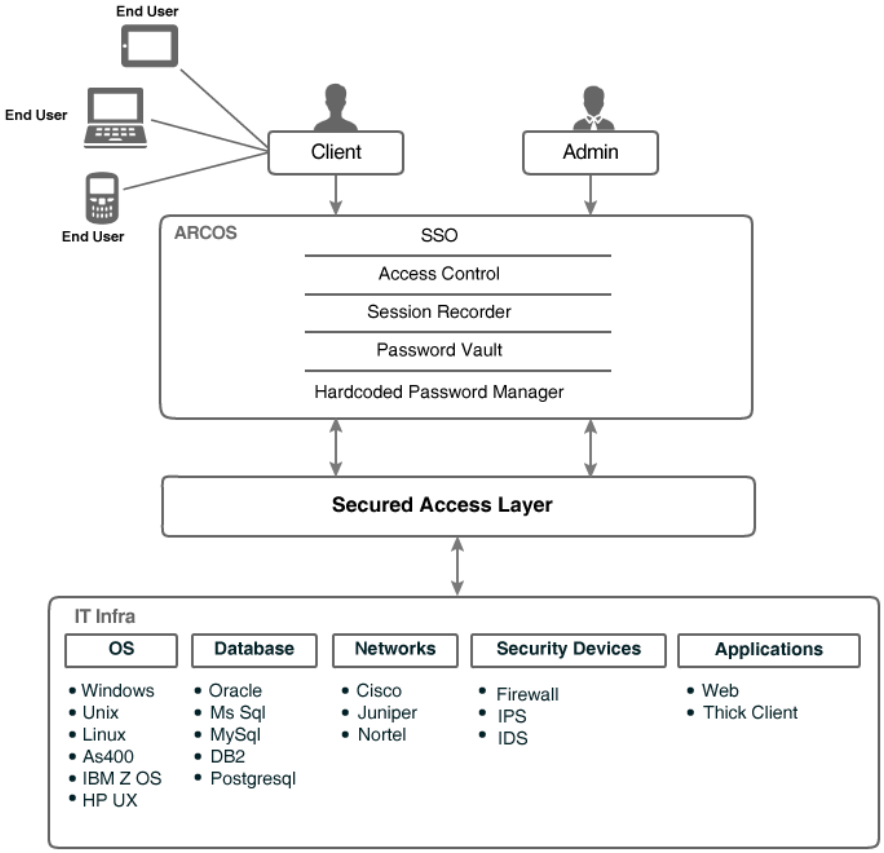

Рис.2.2. Архітектура ARCON PAM в інформаційній системі організації [5]

2.2. Компоненти архітектури рішення безпеки привілейованого доступу

Основними компонентами технології ARCON PAM є:

- SSO;
- Access Control;
- Session Recorder;
- Password Vault;

Зазначені компоненти через рівень контролю безпеки дозволяють управляти привілейованими обліковими записами для роботи привілейованих користувачів та сервісів операційними системами, доступом до баз даних, мережею, доступом до додатків безпеки та web-додатками.

SSO (Single Sign-On)

Усі організації, незалежно від їхнього розміру, використовують безліч застосунків, до яких щоденно отримують доступ різні співробітники в різний час. SSO (Single Sign-On) — це система управління доступом, яка дозволяє користувачам автентифікуватися лише один раз для доступу до кількох різних систем. Рішення ARCON SSO забезпечує надійну інтеграцію SSO для всіх мобільних і веб-застосунків, оптимізованих для мобільних платформ, використовуючи стандартну автентифікацію SAML та інші сучасні протоколи.

ARCON SSO діє як централізований механізм для керування ідентифікацією кінцевих користувачів. Централізоване керування забезпечує безпечний доступ до всіх програм з будь-якого місця та в будь-який час.

Рішення безпечно автентифікується з усіма програмами, як у хмарі, так і локально, використовуючи стандартні одноразові протоколи автентифікації на основі маркерів.

ARCON SSO автентифікує особу кінцевого користувача за допомогою кількох стандартних протоколів автентифікації на основі ідентифікації, таких як 0Auth2.0, OpenID Connect (OIDC) і Security Assertion Markup Language (SAML) .

Таким чином, групи безпеки та оцінки ризиків можуть забезпечити певний рівень довіри до доступу привілейованих користувачів, оскільки ці інструменти засвідчують автентифікацію та шифрування разом із авторизацією ідентифікаторів.

ARCON SSO легко інтегрується зі сховищами автентифікації, такими як Microsoft Active Directory (AD) і Lightweight Directory Access Protocol (LDAP).

Загалом, розгорнувши ARCON | SSO, підприємство може досягти балансу між адміністративною ефективністю та керуванням контролем доступу, забезпечуючи безперебійну роботу кінцевого користувача (працівника). Тому розглянемо більш детально як працює технологія єдиного входу

Технологія єдиного входу (Single sign-on SSO) — метод аутентифікації, який дозволяє користувачам безпечно аутентифікуватися одразу в кількох додатках та сайтах, використовуючи один набір облікових даних.

SSO засновано на налаштуванні довірчих відносин між програмою, відомою як провайдер послуг, та системою управління доступами, наприклад, OneLogin.

Такі довірчі стосунки часто базуються на обміні сертифікатом між системою керування доступом та провайдером послуг. Такий сертифікат може використовуватися, щоб позначити ідентифікаційну інформацію, яка надсилається від системи керування доступами провайдеру послуг, таким чином провайдер послуг знатиме, що інформація надходить із надійного джерела. У SSO ідентифікаційні дані набувають форми токенів, що містять ідентифікаційні значення інформації про користувача, такі як email або ім'я користувача.

Порядок авторизації складається з наступних етапів (рис.2.3):

1. Користувач заходить у додаток або на сайт, доступ до якого він хоче отримати, тобто до провайдера послуг.

2. Провайдер послуг відправляє токен, що містить інформацію про користувача (таку як email адресу) системі SSO (так само відомої, як система управління доступами), як частина запиту на автентифікацію користувача.

3. В першу чергу система управління доступами перевіряє, чи був користувач автентифікований до цього моменту. Якщо так, вона надає користувачеві доступ до провайдера послуг, відразу приступаючи до кроку 5.

4. Якщо користувач не авторизувався, йому буде необхідно це зробити, надавши ідентифікаційні дані, потрібні системою керування доступами. Це може бути просто логін і пароль або інші види аутентифікації, наприклад одноразовий пароль (OTP - One-Time Password).

5. Як тільки система управління доступами схвалить ідентифікаційні дані, вона поверне токен провайдеру послуг, підтверджуючи успішну автентифікацію.

6. Цей токен проходить через браузер користувача провайдеру послуг.

7. Токен, отриманий провайдером послуг, підтверджується згідно з довірчими відносинами, встановленими між провайдером послуг та системою керування доступами під час початкового налаштування.

8. Користувачеві надається доступ до провайдера послуг.

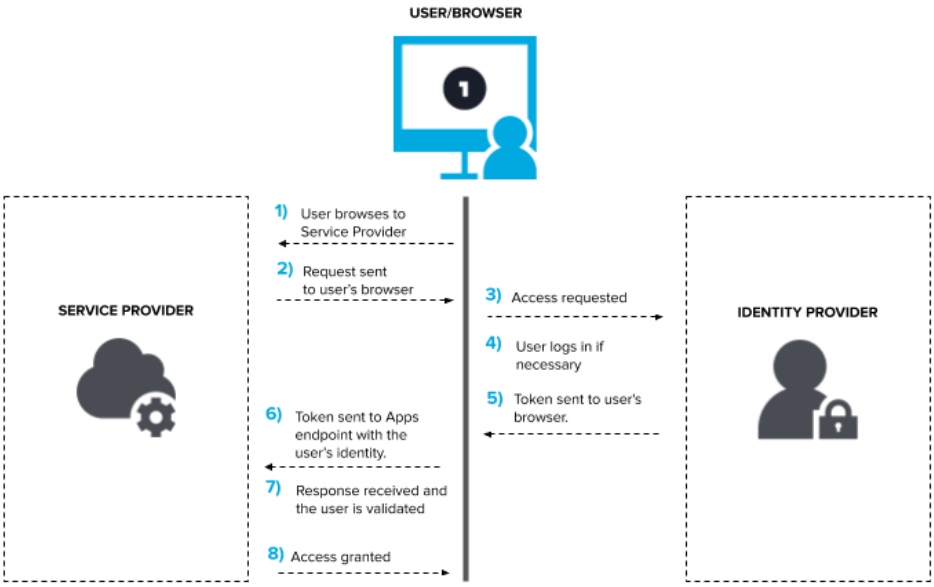

Рис. 2.3. Етапи авторизації в системі SSO

Access Control

ARCON використовує унікальну технологічну структуру, яка надає деталізований контроль доступу для привілейованих користувачів, навіть якщо вони за замовчуванням є суперкористувачами. Це дозволяє обмежити їхній доступ до будь-якої системи, включаючи операційні системи, бази даних, мережеві та безпекові пристрої тощо. Такий детальний контроль доступу допомагає організаціям захищати свої системи від несанкціонованого доступу та випадкових помилок. Він дозволяє обмежувати та контролювати привілейованих користувачів за допомогою централізованої політики, заснованої на правилах та ролях.

Ця функція надає IT-менеджерам з управління ризиками можливості обмеження та фільтрації команд для забезпечення безпечного, санкціонованого та контрольованого доступу до цільових систем. Вона мінімізує ризик, забезпечуючи найглибші рівні деталізованого контролю над обробниками та зберігачами даних.

ARCON Access Control використовує модель контролю доступу RBAC (Role-Based Access Control), де доступ привілейованих користувачів обмежується через ролі й правила. В цій системі користувачам надаються конкретні права доступу

залежно від їхніх ролей у організації, що дозволяє більш чітко контролювати і керувати доступом до системних ресурсів.

Такий підхід допомагає забезпечити безпечний і контрольований доступ, оскільки права та привілеї чітко визначені й розподілені відповідно до ролей.

RBAC – це модель управління доступом, яка базується на присвоєнні користувачам певних ролей. Кожна роль пов'язана з набором дозволів (прав), які визначають, які дії користувач може виконувати в системі. Замість того, щоб надавати дозволи кожному користувачу індивідуально, ми групуємо їх за ролями, що значно спрощує управління доступом і робить його більш безпечним.

Крім RBAC, існують й інші моделі, кожна з яких має свої особливості та області застосування:

Управління доступом на основі атрибутів (ABAC) надає більш детальний контроль доступу, враховуючи різноманітні атрибути суб'єкта, об'єкта і середовища.

Управління доступом на основі контексту (CBAC) визначає доступ на основі контексту, в якому виконується запит (наприклад, час доби, географічне розташування).

Управління доступом на основі політик (PBAC) дозволяє створювати складні політики доступу на основі логічних виразів.

Модель доступу RBAC є важливою для привілейованих користувачів, тому що така модель надає наступні переваги

1. Мінімізує ризики обмежуючи дозволи ролями. Таким чином зменшуємо площу атаки. Якщо зловмисник отримає доступ до облікового запису користувача з обмеженими правами, він зможе виконати менше шкідливих дій.

2. Спрощує управління. Замість того, щоб вручну налаштовувати дозволи для кожного користувача, адміністратори можуть створювати і редагувати ролі. Це значно спрощує процес управління доступом, особливо в великих системах.

3. Високий рівень гнучкості. RBAC дозволяє легко змінювати дозволи користувачів шляхом зміни їхньої ролі. Це особливо корисно, коли користувачі змінюють свої посадові обов'язки.

Порядок роботи моделі RBAC наступний:

Визначення ролей. Спочатку визначаються ролі, які відображають різні функції в організації (наприклад, адміністратор бази даних, розробник, менеджер).

Присвоєння дозволів. Кожній ролі присвоюється набір дозволів, які визначають, які дії користувачі з цією роллю можуть виконувати (наприклад, читання, запис, виконання).

Призначення ролей користувачам. Користувачам присвоюються одна або кілька ролей відповідно до їхніх обов'язків.

Перевірка доступу. При кожній спробі виконання дії система перевіряє, чи має користувач відповідний дозвіл, який пов'язаний з його роллю.

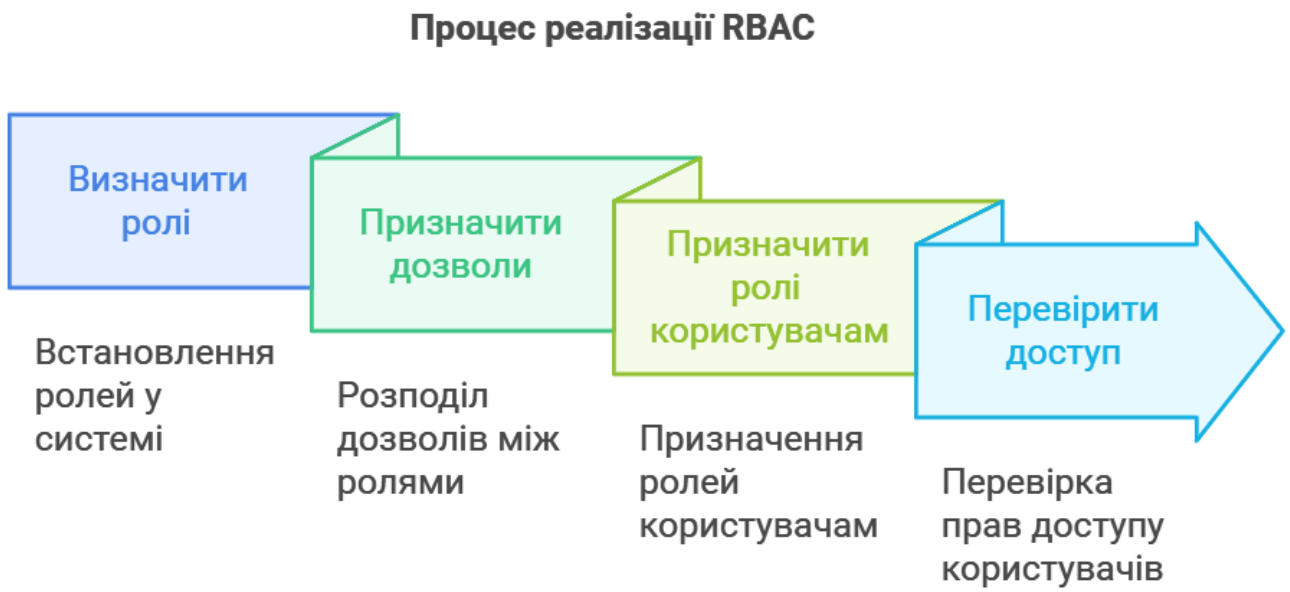

Рис. 2.4. Принцип роботи RBAC

Для ефективного використання RBAC необхідно дотримуватися певних політик (рис.2.5):

Принцип найменших привілеїв. Користувачам надаються тільки ті дозволи, які необхідні для виконання їхніх обов'язків.

Розділення обов'язків. Критичні функції повинні виконуватися кількома користувачами з різними ролями, щоб уникнути конфлікту інтересів.

Регулярний аудит. Необхідно регулярно перевіряти, які користувачі мають які дозволи, і видаляти зайві дозволи.

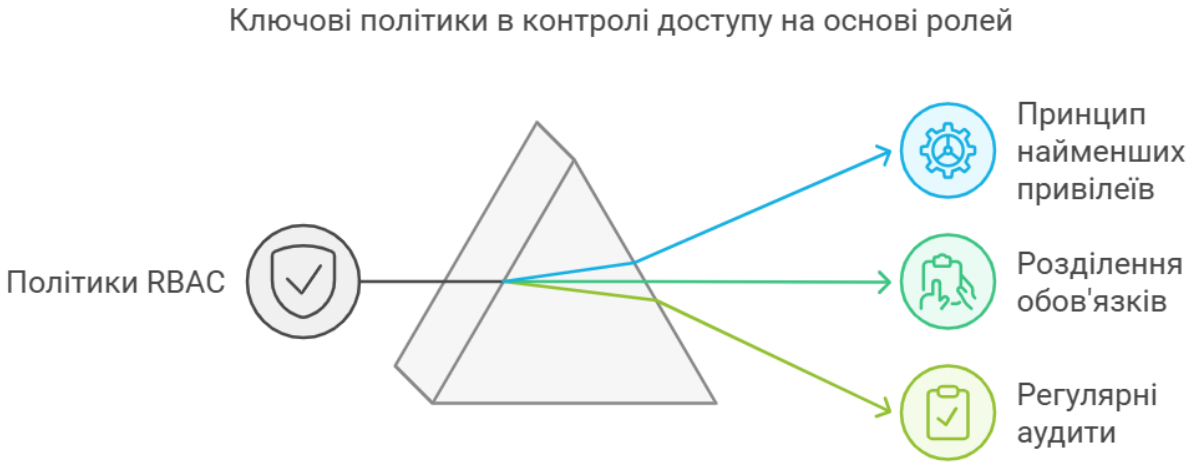

Рис.2.5. Ключові політики RBAC

Session Recorder

ACRON Session Recorder це технологія, яка призначена для запису дій користувачів на комп'ютері. Вона створює детальний журнал усіх взаємодій користувача з системою, включаючи, яке включає:

Кліки мишею. Кожна дія миші фіксується для відтворення.

Натискання клавіш. Реєструється кожна натиснута клавіша, включаючи введення паролів (хоча вони можуть бути замасковані для захисту конфіденційності).

Відкриті програми та файли. Фіксується запуск будь-яких програм та відкриття файлів.

Відвідані веб-сайти. Зберігається історія відвідування веб-сторінок.

Копіювання в буфер обміну. Записується будь-який текст або файли, скопійовані в буфер обміну.

ACRON Session Recorder має широкий спектр застосувань, серед якихвідноситься виявлення загроз, розслідування інцидентів, судові докази,нормативна відповідність, демонстрація процесів.

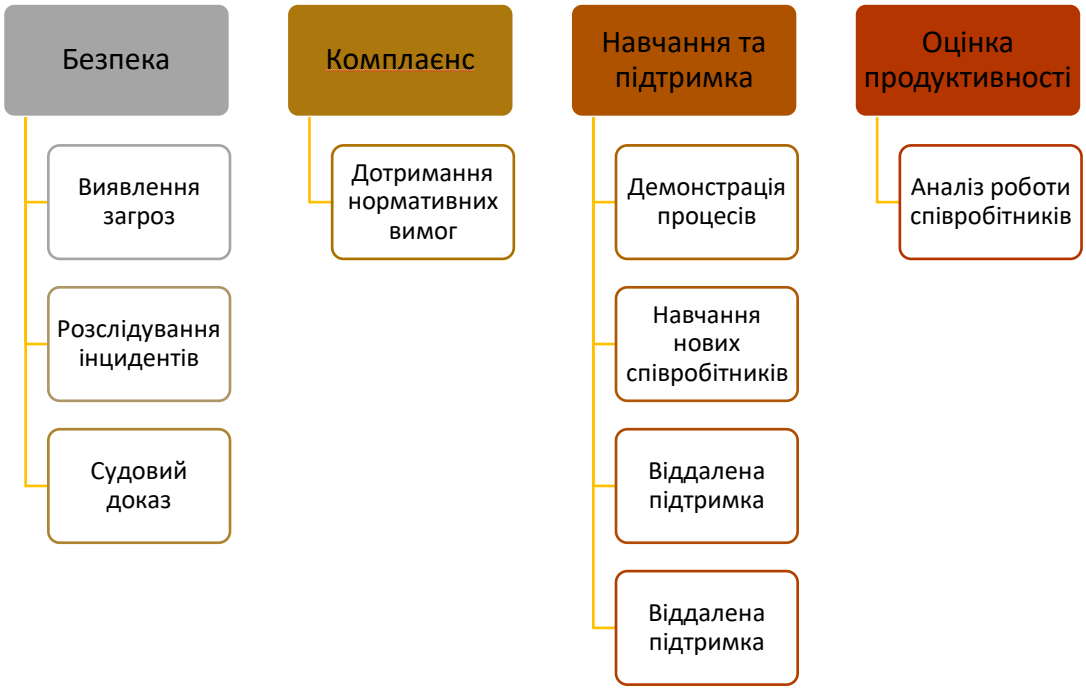

Рис. 2.6. Спектр застосувань ACRON Session Recorder

Виявлення загроз допомагає виявити підозрілу активність користувачів, яка може вказувати на хакерські атаки або внутрішні загрози.

Розслідування інцидентів. Запис сеансів дозволяє детально проаналізувати дії, що призвели до інциденту, і встановити причину.

Судовий доказ. Записи сеансів можуть використовуватися як доказ у судових справах, пов'язаних з кіберзлочинами або іншими правопорушеннями.

Дотримання нормативних вимог. Багато галузей (наприклад, фінансова, медична) мають строгі вимоги до запису дій користувачів для забезпечення безпеки даних. ACRON Session Recorder допомагає дотримуватися цих вимог.

Демонстрація процесів. Записи сеансів можуть бути використані для демонстрації того, як виконуються певні завдання.

Навчання нових співробітників. Записи можуть слугувати як інтерактивні посібники.

Віддалена підтримка. Запис сеансу дозволяє технічним спеціалістам бачити, що відбувається на екрані користувача, і надавати більш ефективну допомогу.

Аналіз роботи співробітників: Записи можуть бути використані для оцінки ефективності роботи співробітників та виявлення областей, де можна покращити процеси.

Password Vault

Спеціалізований інструмент або програмне забезпечення, призначене для безпечного зберігання та управління паролями.

Типові функції Password Vault:

Основна функція Password Vault – це надійне зберігання великої кількості паролів від різних сайтів, програм та облікових записів.

Password Vault генерує сильні паролі. Багато менеджерів паролів мають вбудовані генератори, які створюють складні та унікальні паролі, що важко зламати.

Автоматичне заповнення форм дозволяє автоматично вводити логіни та паролі на веб-сайтах, що значно спрощує процес авторизації.

Для зручного доступу з будь-якого місця надається функція синхронізації між пристроями. Така можливість синхронізує паролі між різними пристроями (комп'ютер, смартфон, планшет) для зручного доступу з будь-де.

Категоризація паролів надає можливість організувати паролі за категоріями (наприклад, соціальні мережі, банківські рахунки, пошта) для зручного пошуку і надання відповідних привілеїв.

Для організації важливим питанням є підвищенням рівня безпеки, тому для привілейованих обдікових запитів обов’язково впроваджується двофакторна аутентифікація. Деякі менеджери паролів підтримують додаткові рівні захисту, такі як двофакторна аутентифікація для підвищення безпеки.

Реалізація управління привілейованим доступом до інформаційної системи організації полягає у створенні єдиної консолі управління для адміністратора безпеки, який зможе управляти всіма доступами, з метою перевірки відповідності привілейованих облікових записів політиці організації, аудиту безпеки, виявлення інцидентів порушення.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1 Варіант технології використання єдиної консолі управління привілейованим доступом ARCON PAM

Технологія у правління привілейованим доступом полягає у використання єдиної консолі, яка дозволяє управляти всіма привілейованими обліковими записам. Це дозволить виявляти нові облікові записи, кількість активних записів, створювати групи облікових записів до відповідних ролей, які внесені до системи управління привілейованого доступу.

Рис.3.1. Консоль ARCON PAM

Панель управління активами ARCON PAM надає адміністраторам безпеки візуальний огляд стану та використання різних привілейованих активів у

інформаційній системі організації. Вона дозволяє швидко оцінити ключові показники та прийняти обґрунтовані рішення.

Основні елементи панелі:

У верхній частині панелі знаходиться меню навігації, яке дозволяє переходити між різними розділами системи.

До основних розділів системи належить :

Infrastructure Asset - загальна кількість інфраструктурних активів.

Total Privilege Account - загальна кількість привілейованих облікових записів.

Total Services - загальна кількість сервісів.

Live Asset -кількість активних активів.

Графіки та діаграми, які зображено на рис 3.2.:

Top 5 Most Used Asset. Діаграма показує топ-5 активів, що найбільш використовуються за певний період.

Top 5 Provisioned Asset. Діаграма демонструє топ-5 активів, що були надані або налаштовані.

Asset Status. Кругова діаграма відображає загальний стан усіх активів.

Service Type. Кругова діаграма показує розподіл активів за типами сервісів.

Ця панель надає інформацію адміністратору безпеки про загальний стан системи, використання активів, стан сервисів, потенційні проблеми.

Загальний стан системи. Панель дає швидке уявлення про масштаб системи, кількість активів та їх використання.

Використання активів. Дозволяє ідентифікувати найпопулярніші активи, які найменш використовуються.

Стан сервісів. Демонструє, які сервіси найактивніші та які типи сервісів переважають.

Потенційні проблеми. Можуть виявити проблеми, такі як активи, що не використовуються, перевантажені сервіси або високий рівень привілейованих облікових записів.

Використовуючи та аналізуючи дані цієї панелі до зволяють адміністраторам безпеки може проводити різні дії.

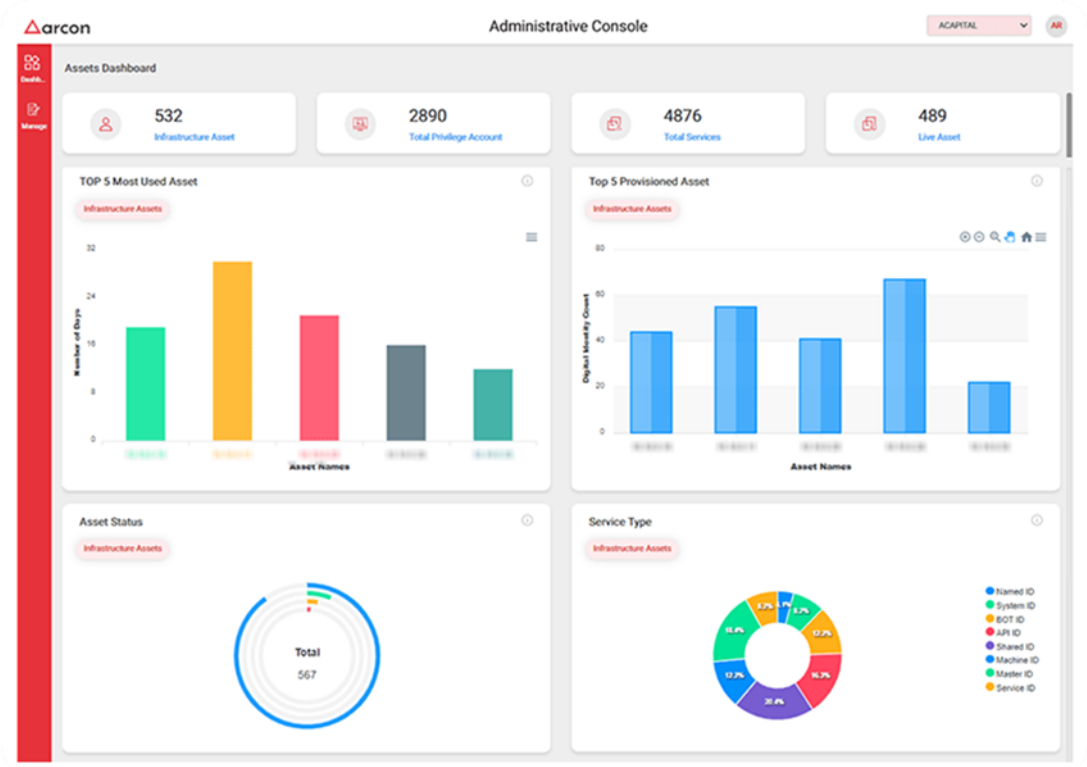

Рис. 3.2. Панель управління активами

Вивчення даних з панелі дозволяє приймати рішення про оптимізацію ресурсів, покращення продуктивності та підвищення безпеки.

За підсумками отриманої інформації можна планувати розширення системи, оновлення устаткування чи зміна конфігурації сервісів.

Панель може допомогти швидко ідентифікувати проблеми та вжити заходів для їх усунення.

Дані з панелі можна використовувати для створення звітів для посібника або інших зацікавлених осіб.

В залежності від функціоналу системи ARCON панель може надавати додаткові можливості, такі як:

Можливість фільтрування даних за різними критеріями (тип активу, дата, статус).

Можливість сортувати дані за різними параметрами.

Можливість експортувати дані до різних форматів для подальшого аналізу.

Можливість налаштувати віджети та графіки відповідно до індивідуальних потреб.

Панель управління активами ARCON PAM є важливим інструментом для адміністраторів, що дозволяє ефективно управляти та контролювати IT-інфраструктуру. Вона надає цінну інформацію для прийняття обґрунтованих рішень та оптимізації роботи системи.

Панель управління ARCON Vault

Панель управління системою зберігання та управління паролями ARCON Vault. Панель надає детальний огляд стану системи, включаючи інформацію про вік паролів, успішність ротації паролів, способи друку інформації з паролями та найчастіші запити на отримання паролів (рис.3.3).

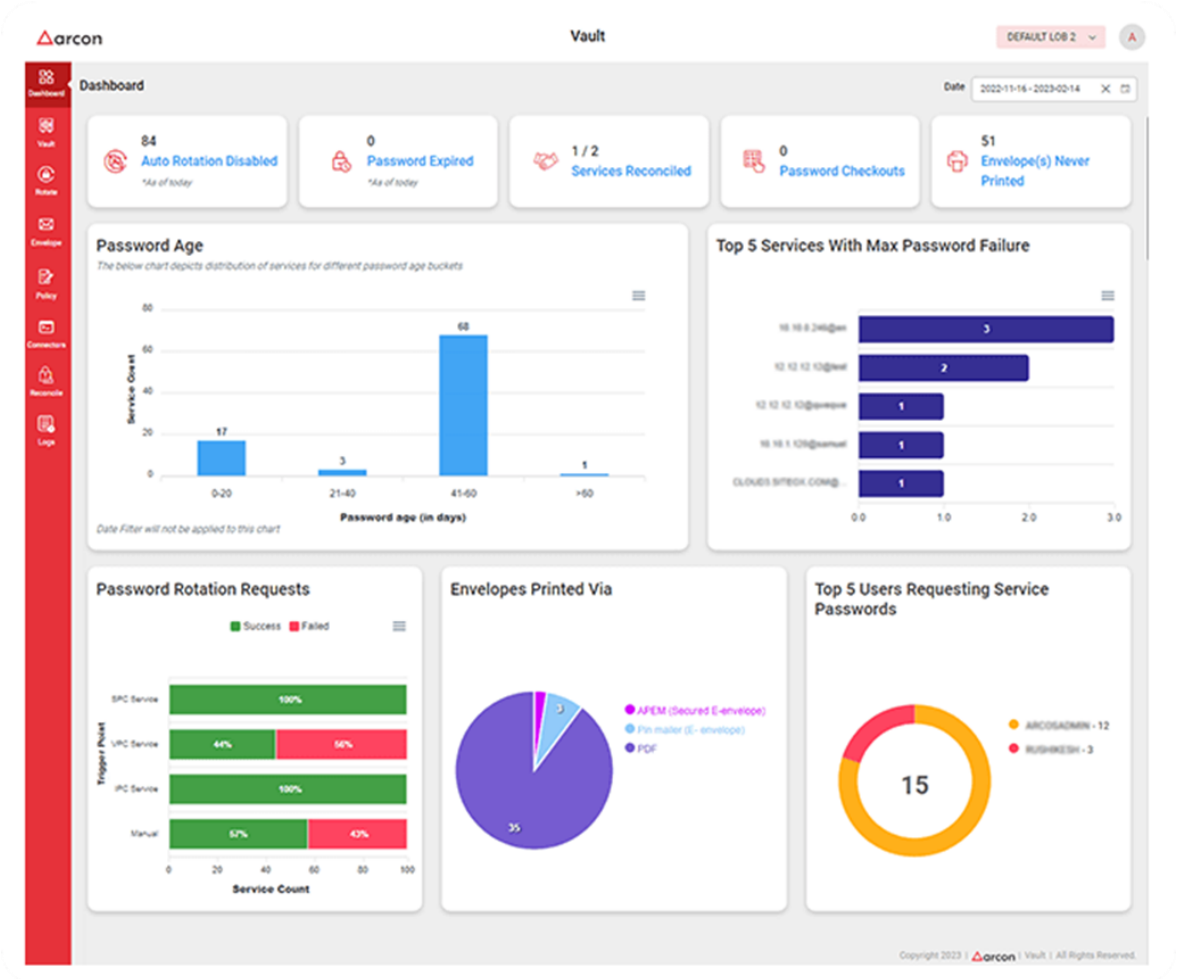

Рис.3.3. Панель управління ARCON Vault

Основні розділи цієї панелі включають:

Auto Rotation Disabled: Кількість сервісів, для яких автоматична ротація паролів вимкнена.

Password Expired: Кількість паролів, у яких вже закінчився термін дії.

Services Reconciled: Кількість сервісів, для яких була виконана звірка паролів.

Password Checkouts: Кількість випадків, коли користувачі вилучали паролі.

Envelopes Printed: Кількість надрукованих листів з паролями.

Завдяки панелі управління ARCON Vault є можливість отримати наступні інформаційні діаграми:

Password Age: Гістограма показує розподіл сервісів за віком паролів. Це дозволяє оцінити, наскільки регулярно оновлюються паролі.

Top 5 Services With Max Password Failure: Діаграма показує топ-5 сервісів, для яких було найбільше невдалих спроб зміни паролів.

Password Rotation Requests: Діаграма показує успішність запитів на ротацію паролів для різних типів сервісів.

Envelopes Printed Via: Кругова діаграма показує, яким чином друкувалися файли з паролями (електронний документ, PDF, фізичний друк).

Top 5 Users Requesting Service Passwords: Кругова діаграма показує топ-5 користувачів, які найчастіше запитували паролі.

Використання цієї панелі надає абмініструторам безпеки дізнатись про загальний стан безпеки, якість паролів, ефективність процесів, поведінку користувачів

Загальний стан системи. Панель дає швидке уявлення про те, наскільки добре працює система управління паролями, скільки паролів потребує оновлення, які сервіси є найбільш проблемними тощо.

Якість паролів За даними про вік паролів можна оцінити, наскільки часто оновлюються паролі і чи відповідають вони політиці безпеки оранізації.

Ефективність процесів. Інформація про успішність ротації паролів, кількість невдалих спроб і способи друку файлів допомагає оцінити ефективність роботи системи.

Поведінка користувачів. Аналіз даних про запити на паролі дозволяє зрозуміти, які користувачі найбільш активні і які сервіси є найбільш затребуваними.

Адміністратор безпеки використовуючі інформацію з цієї панелі може проводити аналіз даних, оптимізувати процеси, усувати проблеми, створювати звіти.

Детальний аналіз даних з панелі дозволяє виявити проблеми, такі як старі паролі, часті невдалі спроби зміни паролів, нераціональне використання функціоналу системи.

На основі отриманих даних можна внести зміни в конфігурацію системи, наприклад, змінити політику ротації паролів, налаштувати автоматичні сповіщення про закінчення терміну дії паролів.

Панель допомагає швидко виявити і усунути проблеми, пов'язані з управлінням паролями.

Дані з панелі можуть бути використані для створення звітів для керівництва або аудиторів.

Отже, панель управління ARCON Vault є потужним інструментом для забезпечення безпеки паролів. Вона дозволяє адміністраторам контролювати стан системи, виявляти потенційні проблеми та вживати заходів для їх усунення.

3.2. Технологія організації заміни паролів для привілейованих облікових записів

Заміна паролів для привілейованих облікових записів є критично важливим аспектом кібербезпеки будь-якої організації. Ці облікові записи надають доступ до чутливих даних та систем, тому їх захист має бути пріоритетом. Дана технологія пропонує детальний план організації цього процесу на прикладі облікового запису адміністратора та облікового запису сервера.

Технологія організації зміни паролів повинен включати наступні етапи для підвищення ефективності управління привілейованим обліковими записами:

1. Розробка політики зміни паролів (рис.3.5)
2. Вибір інструментів (рис.3.6)
3. Процес зміни паролів (рис.3.7)
4. Контроль та аудит (рис.3.8)
5. Робота з користувачами (рис.3.9)

Рис.3.4. Етапи технології зміни паролів

1. Розробка політики зміни паролів

Періодичність зміни: Визначте чіткі строки, з якою частотою потрібно змінювати паролі. Рекомендується змінювати паролі для адміністраторів щоквартально, а для серверів – щорічно.

Складність паролів: Встановіть вимоги до складності паролів: мінімальна довжина, обов'язкова наявність великих і малих літер, цифр та спеціальних символів.

Заборона повторних паролів: Забороніть використання паролів, які використовувалися раніше.

Зберігання паролів: Визначте, хто і як буде зберігати нові паролі. Рекомендується використовувати надійний менеджер паролів.

Процедура зміни паролів: Розробіть детальний алгоритм дій для зміни паролів, включаючи відповідальних осіб та їхні ролі.

Рис. 3.5. Розробка політик паролів

2. Вибір інструментів

Менеджер паролів: Виберіть надійний менеджер паролів для зберігання паролів і генерації нових.

Система управління привілейованим доступом (PAM): Якщо оранізація використовує PAM необхідно використовувати її для автоматизації процесу зміни паролів.

Скрипти: Для автоматизації рутинних завдань можна використовувати скрипти на PowerShell або інших мовах програмування.

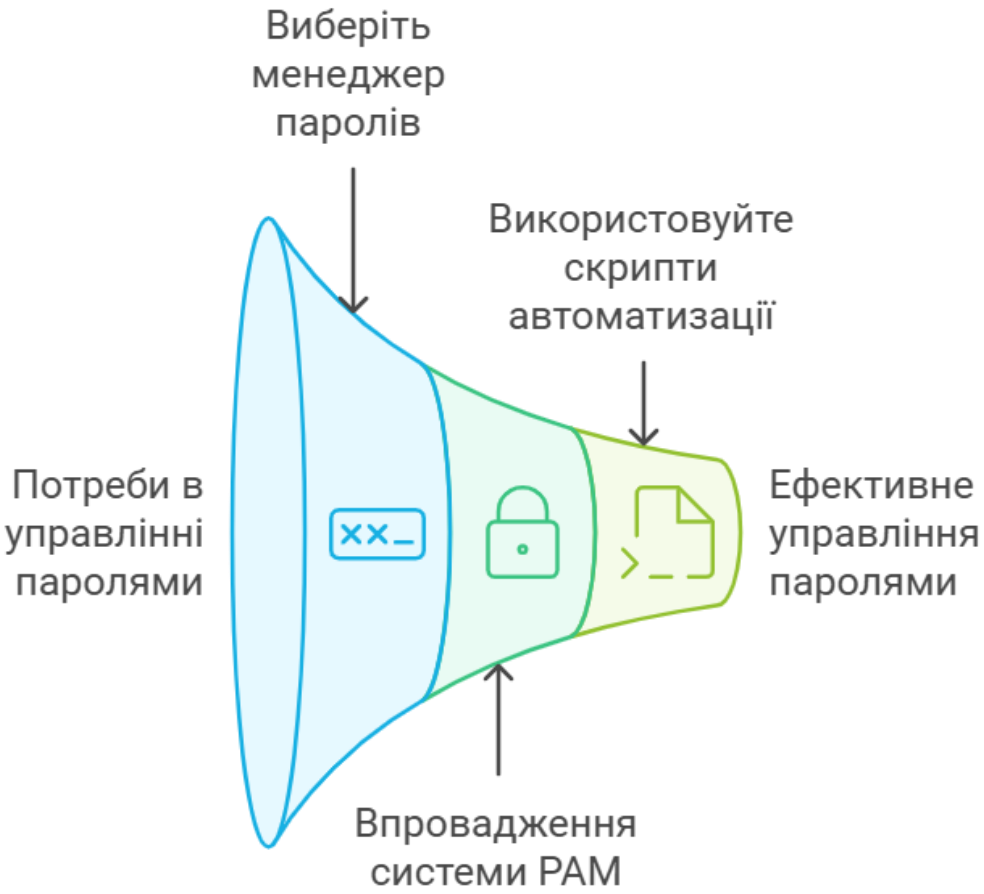

Рис. 3.6. Вибір інструментів

3. Процес зміни паролів

Адміністраторський обліковий запис:

Створіть графік зміни паролів.

Використовуйте генератор паролів для створення нового, сильного паролю.

Змініть пароль в системі управління доступом та всіх службах, де використовується цей обліковий запис.

Запишіть новий пароль у менеджер паролів.

Повідомте про зміну паролю всіх зацікавлених осіб.

Обліковий запис сервера:

Створіть графік зміни паролів.

Використовуйте скрипти для автоматичної зміни паролів в операційній системі та додатках.

Запишіть новий пароль у менеджер паролів.

Перевірте, що всі служби працюють коректно після зміни паролю.

Рис. 3.7. Процес зміни паролів

4. Контроль та аудит

Журналювання: Ведіть журнал всіх змін паролів, включаючи дату, час, користувача, який виконав зміну, старий і новий пароль.

Моніторинг: Регулярно перевіряйте, чи всі паролі були змінені відповідно до встановлених правил.

Аудит: Проводите регулярні аудити системи управління доступом для виявлення потенційних проблем.

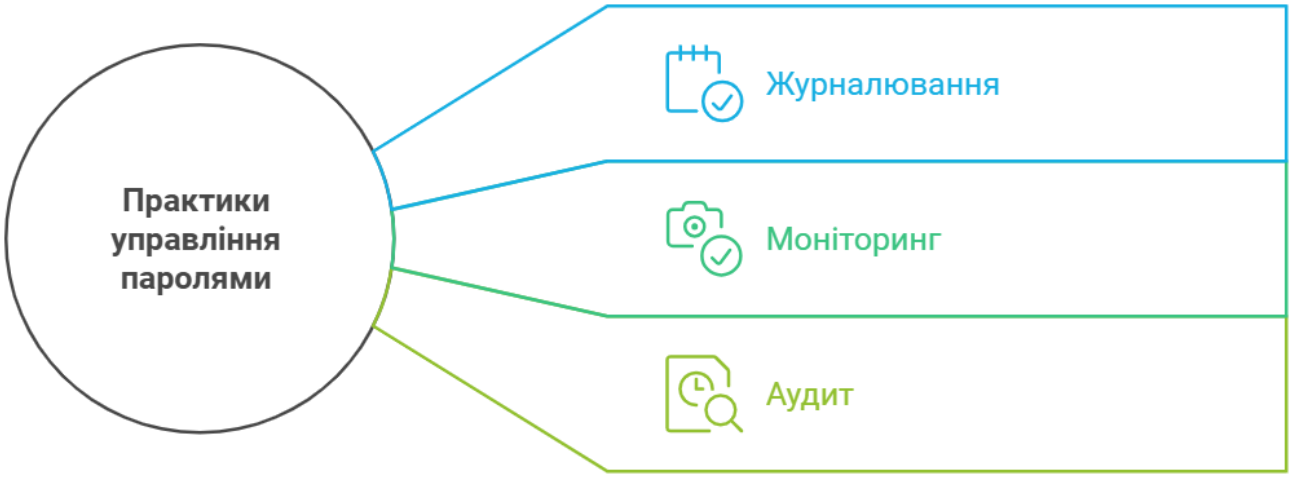

Рис. 3.8. Контроль та аудит

5. Робота з користувачами

Навчання: Проведіть навчання для всіх користувачів, які мають доступ до привілейованих облікових записів. Поясніть їм важливість сильних і унікальних паролів, а також правила зміни паролів.

Політики: Розробіть чітку політику щодо паролів і довести її до відома всіх співробітників.

Рис.3.9. Робота з користувачами

Додатковими рекомендації при створенні паролів для управління привілейованим доступом до інформаційної системи організації повинні включати Рекомендації щодо створення паролів двофакторну аутентифікацю, обмеження доступу та регулярні оновлення.

Двофакторна аутентифікація надає додатковий рівень захисту інформаційної системи від несанкціонованого доступу.

Обов’язково надавати обмеження доступу. Такий підхід надасть привілейованим користувачам мінімальні привілеї, необхідні для виконання їхніх обов'язків.

Необхідно регулярно оновлювати операційні системи, додатки та інструменти безпекиякі зловмисник може використти для до ступу до інформаціної системи.

Обов’язково розробити план реагування на інциденти, які повйязані з порушенням безпеки привілейованого доступу.

Ретельна організація процесу заміни паролів для привілейованих облікових записів є важливим кроком для підвищення рівня безпеки інформаційної системи організації. Дотримання вищезазначених рекомендацій допоможе зменшити ризик несанкціонованого доступу до ваших систем і даних.

3.3. Рекомендації застосування технології управління привілейованим доступом

Управління привілейованим доступом (PAM) забезпечує надійну структуру для захисту та керування привілейованими обліковими записами, забезпечуючи захист конфіденційних облікових даних за допомогою передових методів, таких як сховище облікових даних, автоматичне керування паролями та своєчасний доступ. Застосовуючи суворий контроль доступу, багатофакторну автентифікацію та моніторинг сеансів, рішення PAM мінімізують ризик несанкціонованого доступу та неправильного використання облікових даних. Крім того, аудит у режимі реального часу, політики доступу на основі ролей і підтримка віддаленого доступу

та доступу сторонніх розробників покращують безпеку та відповідність вимогам, пропонуючи комплексний підхід до керування та захисту привілейованих ресурсів.

Інструменти PAM дозволяють автоматизувати та контролювати весь процес надання доступу та паролів привілейованим обліковим записам.

Кожного разу, коли привілейований користувач запитує доступ, система PAM може автоматично генерувати новий пароль, щоб уникнути повторного використання або витоку пароля, одночасно забезпечуючи відповідність між поточними обліковими даними та цільовими системами.

Дуже важливі та конфіденційні облікові дані надаються лише за умови дотримання встановленої політики та отримання всіх необхідних дозволів.

PAM включає обробку дозволів доступу на основі ролей і політик. У своєму рішенні PAM ви можете визначити фіксовану кількість параметрів, які контролюють адміністративний доступ, а також обмежити доступ до певних функцій і ресурсів.

1. Моніторинг і контроль привілейованих сеансів, включаючи запис і аудит дій під час сеансу для виявлення підозрілих дій і реагування на них.

2. Надання привілейованого доступу Just-In-Time (JIT): лише за потреби та протягом обмеженого часу, що зменшує вікно можливостей для зловживання.

3. Багатофакторна автентифікація (MFA) надає застосування додаткових рівнів автентифікації для перевірки ідентичності привілейованих користувачів, що підвищує безпеку за межами просто паролів.

4. Контроль доступу та політики надає визначення та застосування детальних політик доступу на основі ролей, гарантуючи, що користувачі мають мінімально необхідний доступ для виконання своїх обов’язків.

5. Аудит і звітність у реальному часі надає широкі можливості журналювання та звітності для відстеження доступу та активності для відповідності та криміналістичного аналізу.

6. Підтримка віддалених працівників і третіх осіб це коли віддалені працівники та треті сторони повинні мати доступ до систем і даних, необхідних для виконання своєї роботи.

7. Ідентифікаційні дані мають бути консолідовані в усіх операційних системах і середовищах, локальних і хмарних, щоб ви знали, хто з яких облікових записів пов’язаний.

8. Програмне забезпечення PAM повинно надавати сторонньому персоналу рольовий доступ до систем без необхідності введення облікових даних домену, таким чином обмежуючи доступ до привілейованих ресурсів.

9. Підтримка надзвичайних ситуацій. Рішення має давати змогу налаштувати елементи керування доступом і робочі процеси затвердження для сценарію «розбитого скла». Якщо виникає загальна надзвичайна ситуація, користувач може поставити прапорець у системі, щоб вказати, що затвердження не потрібне для будь-якої перевірки. Усі такі запити мають бути підтверджені автоматично, але все одно перевірені, і ви повинні заздалегідь визначити, хто може запитувати такий доступ, хто відповідає за його затвердження та в яких системах.

Інтеграція PAM з існуючою IT-інфраструктурою

Інструменти PAM інтегруються з існуючою IT-інфраструктурою для підвищення безпеки та контролю над привілейованими обліковими записами. Ось основні аспекти різних інтеграцій:

Керування користувачами та автентифікація для PAM дозволяє контролювати та безпечний доступ до критично важливих систем. Основним елементом PAM є керування ідентифікаторами користувачів, забезпечення доступу до привілейованих облікових записів лише авторизованим користувачам, впровадження методів надійної автентифікації, моніторинг дій користувачів і застосування політик для запобігання несанкціонованому доступу та потенційним порушенням безпеки.

PAM має вирішальне значення для захисту критично важливих систем і конфіденційних даних.

Прийняття надійного рішення PAM має важливе значення для захисту конфіденційних систем і даних. Від зберігання облікових даних і керування сеансами до багатофакторної автентифікації та аудиту в реальному часі, інструменти PAM забезпечують комплексні заходи безпеки для захисту

привілейованих облікових записів. Інтегруючи PAM з існуючою IT-інфраструктурою та дотримуючись найкращих практик для керування привілейованими користувачами, організації можуть значно посилити свою безпеку.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Виявлено, що системи організацій часто зазнають атак, спрямованих на отримання доступу до облікових записів з підвищеними правами. Для вирішення цієї проблеми було запропоновано використовувати технологію управління привілейованим доступом (PAM).

Після аналізу різних рішень було обрано технологію ARCON PAM. Ця технологія дозволяє обмежувати доступ до критичних систем лише авторизованим користувачам, запобігає несанкціонованому доступу до конфіденційної інформації, зменшує ризики кібератак, пов'язаних з використанням привілейованих облікових записів, автоматизує багато рутинних завдань, пов'язаних з управлінням доступом.

Розроблена архітектура платформи ARCON PAM забезпечує маштабованість, надійність та гнучкість. Архітектура може бути використана як для невеликих, так і для великих організацій, яка захищає привілейований доступ від різноманітних загроз та легко адаптується до різних потреб організації.

ARCON PAM, яка дозволяє оцінювати стан системи шляхом відстеження активність і виявляти потенційні проблем в інформаційній системі та забезпечує регулярну зміну паролів, що забезпечує безпеку привілейованих облікових записів..

В результаті виконання кваліфікаційної роботи отримано технологію управління привілейованим доступом, яка враховує потреби організації та вимагає мінімальних зусиль для налаштування. Така технологія на відміну від інших може бути повністю функціональною за дуже короткий період часу.

Розроблено рекомендації щодо використання інформаційної панелі ARCON PAM для огляду загального стану системи.

Крім того, надані рекомендації щодо організації безпечної зміни паролів допомагають забезпечити додатковий рівень захисту.

Використання технології ARCON PAM дозволить організації підвищити рівень кібербезпеки та захистити свої дані від несанкціонованого доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1 IBM. (2024, 19 липня). Privileged access management. URL:https://www.ibm.com/think/topics/privileged-access-management (Дата звернення: 12.10.2024).

2. Lewis, S. (2021). privileged access management (PAM). Security. URL: https://www.techtarget.com/searchsecurity/definition/privileged-access-management-PAM (дата звернення: 12.10.2024).

3. Gartner. (2024, November 04). Retrieved from https://www.gartner.com/doc/reprints?id=1-2IRCE33T&ct=240909&st=sb (дата звернення: 20.10.2024).

4. Admin . (2024). What is Privileged Access Management (PAM)? - ARCON. ARCON. Retrieved from https://arconnet.com/what-is-privileged-access-management-pam (дата звернення: 25.10.2024).

5. Privileged Access Management-Arcon - Hermitage Solutions. (2017, November 21). Retrieved from https://www.hermitage.lt/en/news/arcon-privileged-access-management

6. Harris, C. (2024). Discover the top privileged access management solutions. Explore features such as password management, role-based security, real-time notifications, and reporting. Expert Insights. Retrieved from https://expertinsights.com/insights/the-top-privileged-access-management-pam-solutions (дата звернення: 01.11.2024).

7. Blokdyk, G. (2021). Privileged Access Management PAM: A Complete Guide – 2020 Edition [Електронний ресурс]. 5STARCooks.

8. Privileged Identity & Access Management Solution (PAM) Arcon. (2024, September 17). URL: https://arconnet.com/privileged-access-management (дата звернення: 11.11.2024).

9. ARCON PAM Installation and Configuration Guide / Version 4.8.5.0_U4.

10. Koot, A. (2024). Introduction to Privileged Access Management. IDPro Body of Knowledge, 1(13). doi: 10.55621/idpro.101

11. Юхимович А.В., Воротняк М.О., Селітрарь О.О. Підходи до управління привілейованим доступом інформаційної системи організації. *Актуальні проблеми кібербезпеки:* Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Київ, 2024. С. 213-215.