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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM»

зі спеціальності *125 Кібербезпека*
(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

_____ Микола СТЕПАНОВ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
СТЕПАНОВ Микола
(прізвище, ім'я)

Керівник ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф. ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. У контексті забезпечення кібербезпеки та захисту критично важливих інформаційних активів, управління привілейованим доступом (PAM) набуває першочергового значення. Застосування технологій PAM дозволяє суттєво мінімізувати ризики внутрішніх загроз шляхом регламентації доступу до конфіденційних даних та систем виключно для уповноважених осіб, що запобігає потенційним зловживанням. PAM ефективно зменшує поверхню атаки з боку зовнішніх зловмисників, які часто націлені на привілейовані облікові записи як шлях до компрометації інформаційних систем організацій. Впровадження PAM також є необхідною умовою для дотримання вимог законодавства у сфері захисту персональних даних, таких як Закон України, GDPR та PCI DSS, що передбачають жорсткий контроль доступу та моніторинг. Реалізуючи принцип найменших привілеїв та забезпечуючи комплексне керування обліковими записами, PAM обмежує потенційний вплив інцидентів безпеки. Функціональність моніторингу та реєстрації привілейованих сеансів у режимі реального часу забезпечує своєчасне виявлення аномальної активності та можливість проведення ретельного аналізу інцидентів. Таким чином, управління привілейованим доступом є критично важливим для забезпечення надійної безпеки інформаційної інфраструктури організації, відповідності регуляторним вимогам та ефективного протистояння широкому спектру загроз.

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

Предмет дослідження – методи та засоби управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM.

Мета роботи розробити варіант застосування системи управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM.

Наукові завдання:

дослідити сутність проблеми управління привілейованим доступом до інформаційної системи організації;

проаналізувати основні підходи до управління привілейованим доступом до інформаційної системи організації;

проаналізувати існуючі рішення управління привілейованим доступом до інформаційної системи організації;

проаналізувати методи та засоби управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM;

запропонувати варіант впровадження системи управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM;

розробити рекомендацій щодо застосування методів та засобів управління привілейованим доступом до інформаційної системи організації.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування системи управління привілейованим доступом до інформаційної системи організації на прикладі Delinea PAM, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми управління привілейованим доступом

Управління привілейованим доступом (PAM - Privileged access management) – це сфера кібербезпеки , яка регулює та захищає привілейовані облікові записи (такі як облікові записи адміністраторів) та привілейовані дії (такі як робота з конфіденційними даними).

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

Користувачі, які не є людьми, такі як комп'ютери, програми та робочі навантаження, також можуть мати підвищені привілеї. Наприклад, автоматизований процес резервного копіювання може мати доступ до конфіденційних файлів і системних налаштувань.

Привілейовані облікові записи є цінними цілями для хакерів, які можуть зловживати своїми правами доступу, щоб викрасти дані та пошкодити критично важливі системи, уникаючи при цьому виявлення. Фактично, викрадення дійсних облікових записів є найпоширенішим вектором кібератак сьогодні, згідно з індексом IBM X-Force Threat Intelligence Index.

Крім цього небезпека може виходити також зсередини організації. Відомо, що співробітники з добрими намірами можуть ділитися особистими даними організації зі сторонніми продуктами штучного інтелекту (ШІ), не знаючи, чи відповідають ці інструменти їхнім потребам безпеки. Про це свідчить те, що 41% співробітників придбали, модифікували або створили технології без відома своєї IT-служби чи команди безпеки, що створює серйозну прогалину в безпеці.

Відповідно статистики близько 80% організацій не впроваджують, або впроваджують частково рішення для управління привілейованим доступом. Бальшість атак мали спільну рису – вони були здійснено з використанням компрометації привілейованих облікових записів. За оцінками аналітиків, до 80% усіх порушень безпеки пов'язані з компрометацією привілейованих облікових записів (рис 1.1).

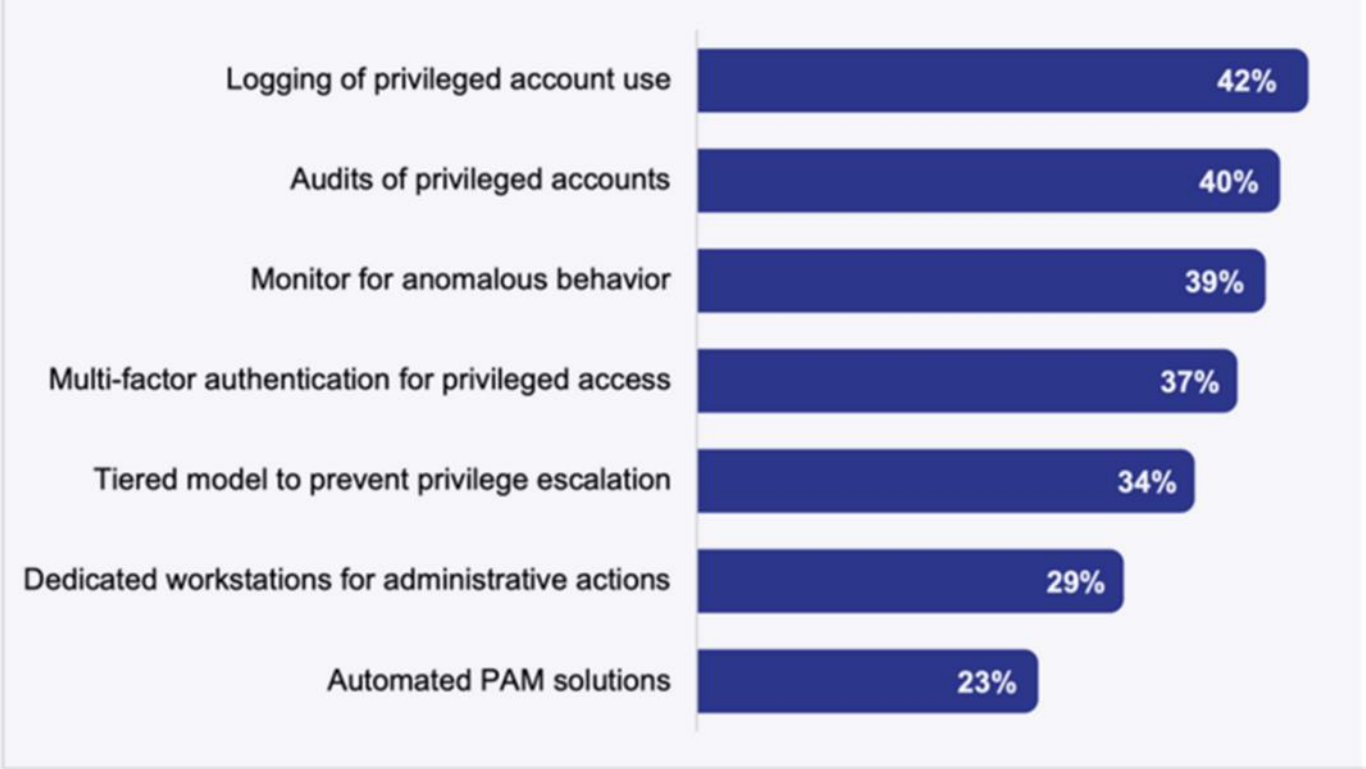

Рис.1.1. Статистика впровадження привілейованих облікових записів в організаціях

Інструменти та практики PAM допомагають організаціям захищати привілейовані облікові записи від атак на основі ідентифікаційних даних. Зокрема, стратегії PAM зміцнюють безпеку організації, зменшуючи кількість привілейованих користувачів та облікових записів, захищаючи привілейовані облікові дані та забезпечуючи дотримання принципу найменших привілеїв.

Керування ідентифікацією та доступом (IAM) – це широка галузь, яка охоплює всі зусилля організації щодо безпеки ідентифікаційних даних для всіх користувачів та ресурсів. PAM – це підмножина IAM, яка зосереджена на захисті

привілейованих облікових записів та користувачів.

На ринку і снує крі PAM ще і IAM рішення. Між ними існує значний збіг. Обидва рішення включають надання цифрових ідентифікацій, впровадження політик контролю доступу та розгортання систем автентифікації та авторизації .

Однак, PAM виходить за рамки стандартних заходів IAM, оскільки привілейовані облікові записи потребують сильнішого захисту, ніж стандартні. Програми PAM використовують розширені заходи безпеки, такі як сховища облікових даних та запис сеансів, щоб суворо контролювати, як користувачі отримують підвищені привілеї та що вони з ними роблять.

Було б непрактично та неефективно застосовувати такі суворі заходи до непривілейованих облікових записів. Ці заходи перервали б доступ звичайних користувачів і ускладнили б виконання людьми своєї повсякденної роботи. Ця різниця у вимогах безпеки є причиною того, що PAM та IAM розійшлися в окремі, але пов'язані дисципліни.

1.2. Аналіз ризиків безпеки привілейованих облікових засобів

Привілейовані облікові записи створюють підвищені ризики для безпеки . Їхні підвищені дозволи є джерелом зловживань, і багато організацій мають труднощі з відстеженням привілейованої активності в локальних та хмарних системах. PAM допомагає організаціям отримати більше контролю над привілейованими обліковими записами, щоб зупинити хакерів , одночасно надаючи користувачам необхідні дозволи.

Атаки на основі ідентифікації, під час яких хакери захоплюють облікові записи користувачів та зловживають їхніми дійсними привілеями, набирають обертів. X-Force від IBM повідомляє , що кількість цих атак зросла на 71% минулого року. Зараз на них припадає 30% порушень безпеки . Ці атаки часто спрямовані на привілейовані облікові записи, безпосередньо або через непрямий рух.

Зловмисники — внутрішні загрози чи зовнішні зловмисники — які отримують доступ до привілейованих облікових записів, можуть завдати серйозної шкоди. Вони можуть використовувати підвищені дозволи для поширення шкідливого програмного забезпечення та доступу до критично важливих ресурсів без обмежень, водночас обманюючи системи безпеки, змушуючи їх вважати законними користувачами з дійсними обліковими записами.

Згідно зі звітом IBM про вартість витоку даних , порушення, під час яких хакери використовують викрадені облікові дані, є одними з найдорожчих і коштують в середньому 4,62 мільйона доларів США. Внутрішні загрози, які зловживають своїми дійсними привілеями, можуть завдати ще більшої шкоди, причому ці порушення коштують у середньому 4,90 мільйона доларів США.

Більше того, цифрова трансформація та розвиток штучного інтелекту збільшили кількість привілейованих користувачів у середньостатистичній мережі. Кожен новий хмарний сервіс, додаток штучного інтелекту, робоча станція та пристрій Інтернету речей (IoT) привносить нові привілейовані облікові записи. Ці облікові записи включають як облікові записи адміністраторів, необхідні користувачам-людям для керування цими активами, так і облікові записи, які ці активи використовують для взаємодії з мережевою інфраструктурою.

Ситуацію ще більше ускладнює те, що люди часто використовують спільні привілейовані облікові записи. Наприклад, замість того, щоб призначати кожному системному адміністратору власний обліковий запис, багато IT-команд створюють один обліковий запис адміністратора для кожної системи та надають доступ до облікових даних користувачам, яким вони потрібні.

В результаті, організаціям важко відстежувати привілейовані облікові записи, поки зловмисники зосереджують свою увагу саме на цих облікових записах.

Технології та стратегії PAM допомагають організаціям отримати кращий огляд та контроль над привілейованими обліковими записами та діями , не порушуючи робочих процесів законних користувачів. Центр інтернет-безпеки

перераховує основні види діяльності PAM до своїх «критично важливих» заходів безпеки.1

Такі інструменти, як сховища облікових даних та своєчасне підвищення привілеїв, можуть забезпечити безпечний доступ для користувачів, яким це необхідно, одночасно запобігаючи проникненню хакерів та неавторизованих інсайдерів. Інструменти моніторингу привілейованих сеансів дозволяють організаціям відстежувати все, що кожен користувач робить зі своїми привілеями в мережі, що дозволяє IT-командам та командам безпеки виявляти підозрілу активність.

Управління привілейованим доступом (PAM) стало критично важливим компонентом захисту конфіденційних даних та IT-систем. Оскільки підприємства прагнуть захистити себе від потенційних порушень, розуміння останньої статистики щодо програмного забезпечення PAM у 2025 році є надзвичайно важливим. Ця статистика дає чітке уявлення про сучасні тенденції, виклики та технологічні досягнення в галузі кібербезпеки, підкреслюючи, як підприємства зміцнюють свій захист від несанкціонованого доступу.

Ключові зацікавлені сторони, включаючи IT-менеджерів, фахівців з кібербезпеки та керівників вищої ланки, вважатимуть ці дані безцінними. Вони розкривають не лише поточний стан галузі, але й прогнозують майбутній розвиток, дозволяючи цим особам, що приймають рішення, удосконалювати свої стратегії безпеки та інвестиційні плани. Висвітлюючи темпи впровадження, показники ефективності та поширені помилки, пов'язані з програмним забезпеченням PAM, статистика надає комплексний огляд, який може допомогти організаціям передбачити та пом'якшити потенційні ризики.

Зрештою, висновки, отримані з цієї статистики, нададуть підприємствам знання, необхідні для прийняття обґрунтованих рішень у галузі, що постійно розвивається. Зі зростанням кіберзагроз повинні розвиватися і підходи до їх запобігання. Цей аналіз на основі даних слугуватиме керівною основою для створення стійких інфраструктур безпеки, гарантуючи, що організації залишатимуться на крок попереду у захисті своїх критично важливих активів.

Розглянемо тенденції та статистику кібербезпеки за 2025 рік.

Майже половина (48,8%) керівників вищої ланки та інших керівних кадрів очікують, що кількість та масштаб кіберподій, спрямованих проти бухгалтерських та фінансових даних їхніх організацій, зростуть у наступному році [3].

Майже 20,3% опитаних керівників стверджують, що бухгалтерські та фінансові команди їхніх організацій тісно та послідовно співпрацюють зі своїми колегами у сфері кібербезпеки [3].

Міжнародна корпорація даних стверджує, що ринок штучного інтелекту на ринку кібербезпеки зростає зі середньорічним темпом зростання (CAGR) на рівні 23,6% і досягне ринкової вартості 46,3 мільярда доларів у 2025 році [3].

За прогнозами Cybersecurity Ventures, збитки від кіберзлочинності досягнуть 8 трильйонів доларів у 2025 році та зростуть до 10,5 трильйонів доларів до 2025 року [3].

За даними дослідників Synopsys, принаймні одна вразливість з відкритим кодом була виявлена у 84% кодових баз [3].

91% кодових баз, досліджених дослідниками Synopsys, містили застарілі версії компонентів з відкритим кодом [3]

Громадські системи охорони здоров'я (CHS) підтвердили, що хакери-злочинці отримали доступ до особистої та захищеної медичної інформації щонайменше 1 мільйона пацієнтів [3].

Найвищий рівень мобільного фішингу в історії спостерігався у 2025 році, коли половина власників мобільних телефонів у всьому світі щоквартально піддавалися фішинговій атаці [3].

Фішингові атаки, що не стосуються електронної пошти, поширюються, причому кількість атак, пов'язаних з вішингом (голосовий фішинг), смішингом (SMS-фішинг) та квішингом (фішинг QR-кодів), зросла в сім разів у другому кварталі 2025 року [3].

Потенційний щорічний фінансовий вплив мобільного фішингу на організацію з 5000 співробітників становить майже 4 мільйони доларів. [3]

У 2025 році 76% організацій стали мішенню атаки програм-вимагачів, з яких 64% були фактично заражені [3].

Лише 50% цих організацій змогли повернути свої дані після сплати викупу [3].

78% випадків компрометації ділової електронної пошти (BEC) стосувалися фальшивих листів генеральних директорів з використанням поширених фраз генеральних директорів, що призвело до зростання на 64% з третього по четвертий квартал 2025 року [3].

Розглянемо типові вектори атак на сервери

Зловмисники мають три поширені шляхи доступу до сервера, деякі з яких легше використати, ніж інші, залежно від обставин. Кожен шлях має різні наслідки для безпеки сервера.

Шлях атаки 1: Атаки на сервер через робочі станції користувачів .

Оскільки співробітники працюють віддалено, а організації впроваджують все більше хмарних сервісів для їхньої підтримки, площа цієї атаки ширша, ніж будь-коли. Будь-яка атака, яка отримує доступ до робочої станції користувача (фішинг все ще є поширеним методом), надає зловмиснику плацдарм і трамплін у мережу серверів. Поширена погана практика надання користувачеві доступу до локального облікового запису адміністратора (для встановлення програм, принтерів тощо) грає на руку зловмиснику. Маючи цей привілейований обліковий запис, зловмисник володіє робочою станцією та може максимально її використовувати. Без належного контролю безпеки сервера зловмисник може встановлювати хакерські інструменти та вертикально переміщатися з робочих станцій на сервери.

Шлях атаки 2: Атаки на сервер через сховище паролів споживчого класу .

Деякі організації покладаються на слабкі сховища паролів споживчого класу, які створюють хибне відчуття безпеки. Однак не всі сховища однакові. Якщо сховище не захищене належним чином, а користувача атакують фішинговими атаками або інсайдер вдається до зловмисних дій, зловмисник може отримати доступ до сервера. Якщо зловмисник обійде сховище, він також обійде засоби

контролю доступу та можливості запису сеансів. Це ускладнює для криміналістів пошук джерела атаки.

Шлях атаки 3: Сервер атакує безпосередньо на сервер .

Невдоволені співробітники можуть легко обійти робочі станції кінцевих користувачів і перейти одразу до сервера, незалежно від того, чи знаходиться цей сервер у хмарі, чи локально . Зловмисник, який вже знаходиться в мережі та має відповідні привілеї, спробує перейти від сервера до сервера, щоб отримати доступ до конфіденційних даних та викрасти їх або зашифрувати для отримання викупу.

Отже, організаціям необхідно впроваджувати стратегію архітектури PAM, для захисту своїх важливих ресурсів та активів.

1.3. Аналіз підходів до управління привілейованим доступом

Управління привілейованим доступом поєднує процеси та технологічні інструменти для контролю того, як привілеї призначаються, отримуються та використовуються. Багато стратегій PAM зосереджені на трьох основах:

Керування привілейованими обліковими записами - створення, надання та безпечне видалення облікових записів із підвищеними правами доступу.

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

Керування привілейованими сеансами - моніторинг привілейованої активності для виявлення підозрілої поведінки та забезпечення відповідності вимогам.

В основі привілейованого управління обліковими записами є керування привілейованими обліковими записами, яке контролює весь життєвий цикл облікових записів із підвищеними правами доступу, від створення до виведення з експлуатації.

Надаймо визначення привілейованого облікового запису.

Привілейований обліковий запис – це будь-який обліковий запис із правами доступу, вищими за середні, в системі. Користувачі привілейованих облікових

записів можуть виконувати такі дії, як зміна системних налаштувань, встановлення нового програмного забезпечення та додавання або видалення інших користувачів.

У сучасних IT-середовищах привілейовані облікові записи можуть мати різні форми. Привілейовані облікові записи можуть мати як користувачі-люди, так і інші користувачі, такі як пристрої Інтернету речей та автоматизовані робочі процеси. Приклади включають:

Локальні облікові записи адміністраторів надають користувачам контроль над одним ноутбуком, сервером або іншою окремою кінцевою точкою.

Облікові записи адміністраторів домену надають користувачам контроль над усім доменом, наприклад, над усіма користувачами та робочими станціями в домені Microsoft Active Directory.

Привілейовані облікові записи бізнес-користувачів надають користувачам підвищений доступ для цілей, не пов’язаних з IT, наприклад, обліковий запис, який фінансовий працівник використовує для доступу до коштів компанії.

Облікові записи суперкористувачів надають необмежені привілеї в певній системі. У системах Unix та Linux облікові записи суперкористувачів називаються обліковими записами «root». У Microsoft Windows вони називаються обліковими записами «адміністратора».

Облікові записи служб дозволяють програмам та автоматизованим робочим процесам взаємодіяти з операційними системами.

Облікові записи програм дозволяють програмам взаємодіяти одна з одною, здійснювати виклики до інтерфейсів прикладного програмування (API) та виконувати інші важливі функції.

Стратегія PAM — це не просто впровадження інструментів, а всеохоплюючий підхід, що відповідає системі кібербезпеки організації. Вона працює за принципом надання найменших привілеїв, необхідних для виконання завдання, щоб мінімізувати потенційні поверхні атаки. Приділяючи час розумінню, впровадженню та вдосконаленню вашої стратегії PAM, ви готуєте свою організацію до кращого передбачення, запобігання та реагування на постійно мінливий ландшафт кіберзагроз [2].

Стратегія архітектури PAM включає:

1. Формулювання матриці охоплення контролю PAM.
2. Впровадження основних можливостей PAM.
3. Інтеграція додаткових можливостей PAM.
4. Інтеграція PAM-рішень з інструментами SIEM та ITSM.
5. Розробка архітектури стійкості для PAM-рішення.

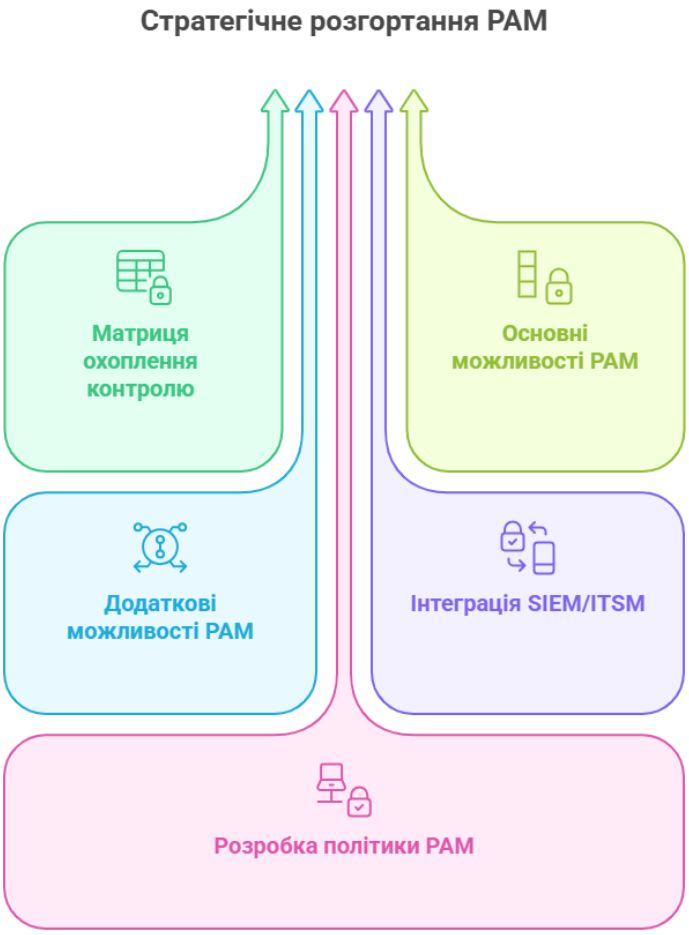

Рис.1.2. Стратегія архітектури PAM

1. Формулювання матриці охоплення контролю PAM

Першим кроком до побудови стійкої стратегії архітектури PAM є формулювання Матриці охоплення засобів контролю PAM. Ця надійна основа прокладає шлях для всеохоплюючої системи кібербезпеки у вашій організації. Матриця являє собою ретельний перелік, що відображає всі привілейовані засоби

контролю доступу, розгорнуті у ваших системах. Вона визначає, де розташовані ці засоби контролю, їхню функціональність та активи, які вони захищають.

Розробка матриці охоплення контролю PAM вимагає глибокого розуміння внутрішнього ландшафту вашої організації та зовнішніх загроз, з якими вона стикається. Вона дозволяє візуалізувати розподіл контролю доступу, виявляти прогалини у вашій системі безпеки та визначати області, що потребують уваги або вдосконалення. Матриця має бути динамічною, забезпечувати часті оновлення та модифікації, враховуючи мінливий характер кіберзагроз. Добре структурована матриця служить компасом, спрямовуючи вашу організацію до досягнення цілей кібербезпеки та підтримки міцної позиції PAM [2] .

2. Реалізація основних можливостей PAM

Після створення Матриці охоплення контролю PAM наступним кроком є впровадження основних можливостей PAM. Ці можливості забезпечують захист від внутрішніх та зовнішніх загроз і формують основу моделі нульових привілеїв. Основні можливості PAM охоплюють управління, виявлення, захист, моніторинг, аудит, а також підвищення та делегування привілеїв «точно в строк» (JIT) [2].

Управління передбачає визначення чітких політик і ролей, тоді як виявлення включає пошук і каталогізацію всіх привілейованих облікових записів у вашій інфраструктурі. Захист гарантує, що ці облікові записи захищені від несанкціонованого доступу, а моніторинг передбачає постійне спостереження за всіма привілейованими діями для виявлення незвичайної поведінки. Аудит передбачає ведення обліку всіх привілейованих доступів та допомогу в розслідуваннях та дотриманні вимог. Підвищення та делегування привілеїв JIT надають привілеї користувачам лише за потреби, мінімізуючи поверхню для атаки [2].

3. Інтеграція додаткових можливостей PAM

Можливості PAM можна розширити шляхом інтеграції додаткових інструментів управління безпекою, які забезпечують більш багаторівневий захист та оптимізовані операційні процеси. До них належать віддалена підтримка для безперебійного доступу, автоматизація завдань для мінімізації помилок, що

виникають вручну, управління змінами для ефективного контролю модифікацій системи, а також оцінка та усунення вразливостей для виявлення та виправлення вразливостей [2].

Керування правами доступу до інфраструктури, ще одна додаткова функція PAM, надає огляд того, хто має доступ до яких ресурсів, забезпечуючи кращий контроль над привілейованими доступами. Цей додатковий рівень можливостей PAM підвищує рівень безпеки організації, допомагає ефективніше керувати ризиками та підвищує загальну операційну ефективність [2].

4. Інтеграція PAM-рішень з інструментами SIEM та ITSM

Ефективна стратегія PAM також інтегрує PAM-рішення з інструментами інформації про безпеку, управління подіями (SIEM) та управління IT-послугами (ITSM). Інструменти SIEM забезпечують аналіз сповіщень про безпеку в режимі реального часу, допомагаючи виявляти потенційні інциденти безпеки. Вони збирають дані журналів та подій з різних джерел, виявляючи закономірності та сигналізуючи про сповіщення про незвичайну активність [2].

З іншого боку, інструменти ITSM обробляють усі процеси, пов'язані з наданням IT-послуг в організації. Коли рішення PAM інтегровані з SIEM та ITSM, безперебійний потік інформації покращує час реагування на інциденти та зменшує ризик порушень безпеки. Така інтеграція також допомагає підтримувати загальний стан системи та підвищує продуктивність [2].

5. Розробка архітектури стійкості для PAM-рішення

Останнім кроком у розробці ефективної стратегії архітектури PAM є розробка архітектури стійкості для PAM-рішення. Це включає створення високодоступного (HA) дизайну та впровадження передових процесів аварійного відновлення. HA-проект гарантує, що ваше PAM-рішення залишається доступним навіть у разі збою деяких компонентів, а передові процеси аварійного відновлення захищають від втрати даних під час катастрофи.

Крім того, планування сценаріїв відновлення з використанням надійних методів швидкого реагування гарантує вам екстрений доступ до критично важливих систем у кризових ситуаціях. Впровадження стійкості у ваше PAM-

рішення захищає вашу організацію від очікуваних та неочікуваних загроз, гарантуючи, що ваші критично важливі системи можуть швидко відновитися та повернутися до нормального режиму роботи [2].

1.4. Аналіз існуючих рішень управління привілейованим доступом до інформаційної системи організації

Організації зазвичай вибудовують багаторівневу структуру своїх систем, де кожен рівень відповідає масштабу можливих негативних наслідків у випадку інциденту безпеки. Зрозуміло, що чим вищий рівень системи, тим катастрофічнішими можуть бути наслідки її неправомірного використання [16].

Для мінімізації таких ризиків використовуються рішення для управління привілейованим доступом (PAM). Вони дозволяють IT-службам та службам безпеки точно регулювати, хто і коли отримує доступ до систем з високим рівнем критичності. Ключовий принцип тут – «доступ за потребою», коли користувачі отримують розширені повноваження лише на той час, який потрібен для виконання конкретного завдання. Після завершення роботи або закінчення встановленого терміну ці права автоматично анулюються. Це не тільки надійно захищає життєво важливі активи компанії від несанкціонованого втручання, але й сприяє більш ефективному дотриманню нормативних вимог у сфері захисту інформації [16].

Розглянемо найбільш відомі рішення привілейованого доступу.

ARCON PAM. ARCON є глобальним постачальником рішень для управління привілейованим доступом. Їхній пакет продуктів зосереджений на наданні надійного захисту, моніторингу та управління привілейованими обліковими записами. ARCON відомий своїм підходом до безпеки на основі ризиків та зручним інтерфейсом. Вони пропонують такі функції, як сховище паролів, управління сеансами, контроль доступу на основі ролей та аналітика загроз [12].

BeyondTrust. BeyondTrust пропонує комплексну платформу для управління привілейованим доступом, яка охоплює управління паролями та обліковими даними, безпечний віддалений доступ та управління привілеями для кінцевих

точок. Їхні рішення спрямовані на зменшення поверхні атаки та запобігання витоку даних, пов'язаних з привілейованим доступом. BeyondTrust часто відзначають за широту функціоналу та інтеграційні можливості [14].

CyberArk. CyberArk є одним із лідерів ринку PAM і пропонує широкий набір рішень для захисту привілейованих облікових записів у локальних, хмарних та гібридних середовищах. Їхня платформа включає безпечне сховище облікових даних, ізоляцію та моніторинг привілейованих сеансів, аналітику загроз та автоматизацію життєвого циклу привілеїв. CyberArk відомий своєю надійністю та здатністю працювати у великих, складних організаціях [15].

Delinea. Delinea утворилася в результаті злиття компаній Thycotic та Centrify. Вони пропонують хмарно-орієнтовані рішення PAM, які забезпечують простий та безпечний доступ для сучасних гібридних підприємств. Delinea фокусується на наданні безшовного та легкого у використанні PAM, який легко інтегрується та масштабується. Їхні рішення охоплюють управління секретами, привілеями сервера та управлінням доступом до хмарних ресурсів [17].

Таблиця 1.1.

Порівняльна таблиця PAM рішень

Характеристика	**ARCON PAM**	**BeyondTrust**	**CyberArk**	**Delinea**
Основний фокус	Надійний захист та управління ризиками	Комплексне управління привілеями та доступом	Захист привілейованих акаунтів у складних середовищах	**Безшовний та простий у використанні PAM для сучасних гібридних підприємств**
Розгортання	Локально, хмара	Локально, хмара, гібридно	Локально, хмара, гібридно	**Переважно хмарно-орієнтований, легке розгортання та масштабування**

Зручність використання	Дружній інтерфейс	Широкий функціонал, може потребувати налаштування	Потужний, але може бути складним для менших команд	**Висока зручність використання, інтуїтивний інтерфейс, швидке впровадження**
Інтеграції	Стандартні інтеграції	Широкі інтеграційні можливості	Розгалужені інтеграції, особливо для великих підприємств	**Легка інтеграція з хмарними сервісами та DevOps інструментами**
Ключові переваги	Управління на основі ризиків, звітність	Широта платформи, управління кінцевими точками	Найвища безпека, лідер ринку, масштабованість для великих організацій	**Простота, гнучкість, хмарна архітектура, швидка окупність інвестицій (ROI), відмінно підходить для середнього та великого бізнесу, що активно використовує хмару**
Підхід до ліцензування	Залежить від модулів	Гнучкі моделі	Може бути комплексним	**Прозоре та гнучке ліцензування, часто вигідніше для хмарних сценаріїв**
Інновації	Постійний розвиток функціоналу	Розширення платформи новими можливостями	Лідерство в інноваціях безпеки привілеїв	**Фокус на хмарних інноваціях, безшовний досвід користувача, автоматизація**

Отже, Delinea може бути кращим вибором.

Delinea виділяється своїм фокусом на простоті та зручності використання, особливо для організацій, які активно переходять у хмару або вже мають гібридну інфраструктуру. Їх хмарно-орієнтована архітектура забезпечує легке розгортання, масштабування та інтеграцію з сучасними інструментами та сервісами. Це часто призводить до швидшої окупності інвестицій (ROI) та менших витрат на адміністрування порівняно з деякими більш традиційними та комплексними рішеннями. Для компаній, яким потрібен потужний, але водночас гнучкий та інтуїтивно зрозумілий PAM, що не вимагає тривалого впровадження та складного налаштування, Delinea є оптимальним вибором [17].

Для подальшого дослідження буде розглянуто архітектуру та функції основних компонентів рішення Delinea PAM.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ОРГАНІЗАЦІЇ

2.1. Архітектура платформи Delinea

Платформа Delinea дозволяє організаціям виявляти всі ідентифікаційні дані, призначати відповідні рівні доступу, виявляти порушення та негайно реагувати на загрози ідентифікаційним даним у режимі реального часу [4].

Платформа Delinea являє собою значний крок вперед у сфері управління привілейованим доступом (PAM), пропонуючи єдиний та комплексний огляд усієї екосистеми PAM вашої організації. Розроблена для безперешкодного поширення управління привілейованим доступом на гібридні багатохмарні інфраструктури, платформа Delinea впроваджує адаптивні елементи керування, які дозволяють IT-командам та командам з кібербезпеки швидко захищати облікові дані, мінімізувати поверхню атаки, зменшувати ризики та дотримуватися нормативних вимог [4].

Архітектура платформи Delinea - це динамічна, керована штучним інтелектом та заснована на ризиках платформа, призначена для управління привілейованим доступом та ідентифікаційною безпекою (рис.2.1) [4].

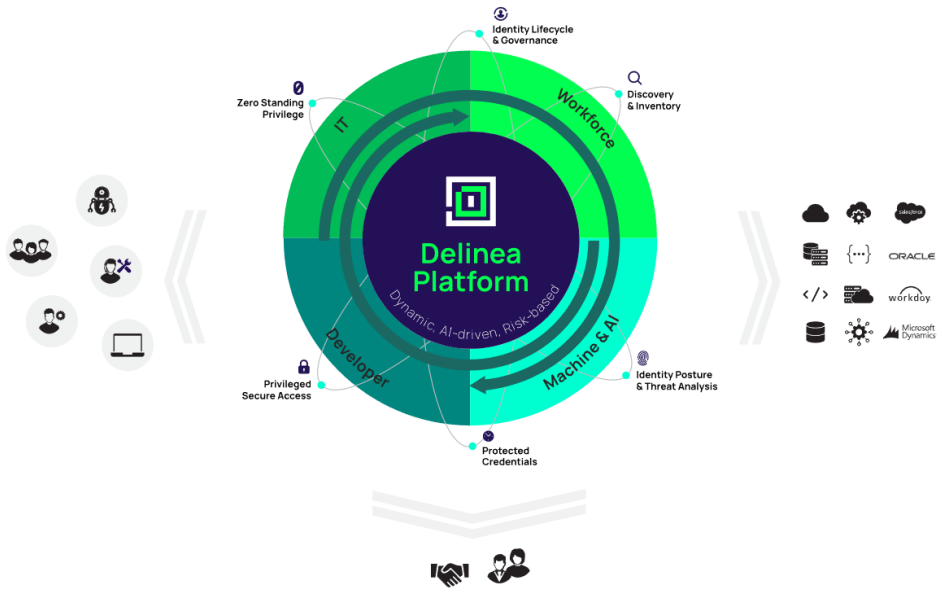

Рис.2.1. Архітектура платформи

Центральним елементом є сама Delinea Platform. Вона функціонує як ядро, забезпечуючи динамічне, кероване штучним інтелектом та засноване на оцінці ризиків управління.

Платформа складається з трьох ключових сегментів взаємодії [4]:

1. IT. Цей сегмент фокусується на інфраструктурі та операціях. Це сегмент виділяє актуальну є концепція *Нульових постійних привілеїв* (Zero Standing Privilege), яка мінімізує ризики шляхом надання доступу лише за необхідності та на обмежений час.

2. Робоча сила (Workforce): Цей сегмент охоплює користувачів та їхній доступ. Ключовими аспектами цього сегментк тут є *Життєвий цикл ідентичностей та управління* (Identity Lifecycle & Governance), а також *Виявлення та інвентаризація* (Discovery & Inventory) для повного розуміння всіх ідентичностей та їхніх прав доступу.

3. *Розробники (*Developer): Для цього сегменту важливим є Захищений привілейований доступ (Privileged Secure Access) до систем та інструментів розробки.

Компонент Машини та ШІ (Machine & AI) відіграє наскрізну роль, забезпечуючи:

- Аналіз стану ідентичностей та загроз (Identity Posture & Threat Analysis), що допомагає виявляти та реагувати на потенційні загрози.
- Захищені облікові дані (Protected Credentials) для машин та додатків.

Взаємодія та інтеграції:

- Ліворуч зображені різні типи суб'єктів взаємодії: роботизовані процеси (автоматизація), групи користувачів (з можливістю привілейованого управління доступом, включаючи блокування), окремі користувачі та кінцеві пристрої/сервери.
- Праворуч показані інтеграції з різними системами та платформами: хмарні провайдери (наприклад, AWS, Azure, GCP), API та власні додатки, бази даних, а також корпоративні системи, такі як Salesforce, Oracle, Workday, Microsoft Dynamics.

Стрілки на діаграмі на архітектурі вказують на циклічний та безперервний характер процесів управління доступом та безпекою, що забезпечуються платформою. Така, архітектура спрямована на забезпечення комплексного та адаптивного підходу до захисту привілейованого доступу в сучасних складних IT-середовищах організацій [4].

Платформа Delinea велику кількість переваг для покращення рівня безпеки до, яких входять наступні показники [17]:

Зменшення ризику. Покращення рівня безпеки організації шляхом захисту привілейованого доступу від входу до підвищення прав, а також проактивне вирішення загроз, пов'язаних з ідентифікацією, та неправильних конфігурацій.

Дотримання вимог відповідності: Адаптивні засоби контролю авторизації та уніфікований аудит спрощують забезпечення дотримання та демонстрацію вимог відповідності.

Централізоване керування. дозволяє керувати привілейованим доступом для спільних облікових даних та всіх ідентифікаційних даних, що охоплюють дані, програми, хмару та традиційну інфраструктуру.

Легке масштабування за своєю програмою PAM. Використовує безпечну хмарну архітектуру Delinea для розвитку організації завдяки безперешкодному впровадженню контролю привілеїв та спільних можливостей.

Швидка окупність інвестицій. Використання майстра налаштування, конфігурації та робочих процесів, дозволяє легко впровадити PAM систему.

При дотриманні всіх рекомендацій при налаштуванні і використанні платформи для організації PAM надають безвідмовну роботу системи на 99,99%.

2.2. Функції менеджера життєвого циклу PAM

Життєвий цикл облікових записів (Account Lifecycle Manager - ALM) контролює створення, керування та виведення з експлуатації облікових записів служби Active Directory, що працюють у мережі організації. ALM зменшує розростання облікових записів служби та підвищує безпеку, забезпечуючи

управління та створюючи підзвітність за допомогою дозволів на основі ролей. Залежно від ролі користувача, він може запитувати, затверджувати, надавати, керувати та виводити з експлуатації облікові записи служби [5].

ALM працює з використанням контролю доступу на основі ролей.

ALM керує обліковими записами служб, призначаючи кожен обліковий запис користувачеві у організації. ALM використовує чотири ролі для визначення дозволів користувачів та визначення відповідальності. Роль користувача визначає, як вони взаємодіють з ALM та обліковими записами служб [5].

До основних ролей відносяться наступні:

Власник облікового запису – усім користувачам ALM надається роль власника облікового запису. Власники облікових записів можуть переглядати та оновлювати керовані облікові записи, призначені їм.

Системний адміністратор – системний адміністратор має повний доступ до налаштування та керування ALM. Він може створювати та керувати користувачами, ролями, групами та робочими процесами.

Запитувач – запитувачі можуть надсилати запити на створення нових облікових записів служби.

Затверджувач – особи, що затверджують, переглядають запити на нові облікові записи служб і затверджують або відхиляють їхнє надання.

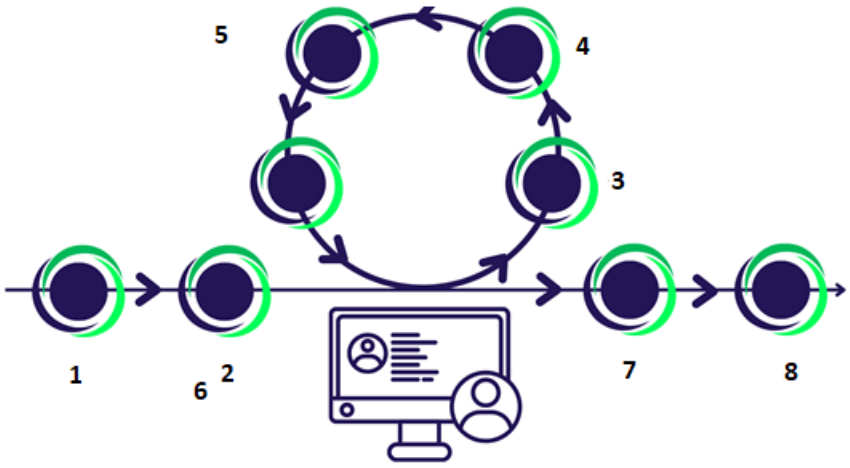

Рис.2.2. Життєвий цикл облікового запису

Життєвий цикл облікового запису охоплює всі етапи існування облікового запису користувача в організації, від моменту приєднання користувача до моменту його виходу. Цей процес є важливим для забезпечення безпеки та належного керування доступом до систем та ресурсів. Хоча цикли можуть дещо відрізнятися для різних типів користувачів, основні принципи залишаються незмінними [5].

Етапи життєвого циклу облікового запису (на прикладі працівника організації):

1. Новий користувач приєднується до організації. Процес починається, коли новий співробітник приходить в організацію. Відповідний запис про нього створюється в системі управління персоналом (HR).
2. Система створює цифрову ідентичність. На основі даних з HR-системи для нового користувача створюється унікальна цифрова ідентичність.
3. Створення облікових записів для всіх необхідних систем. Для нового користувача створюються облікові записи в усіх системах та сервісах, до яких йому потрібен доступ для виконання своїх робочих обов'язків.
4. Зміна ролі користувача. Протягом роботи в організації роль користувача може змінюватися (наприклад, підвищення, переведення в інший відділ). Це вимагає оновлення його прав доступу та, можливо, створення нових або модифікації існуючих облікових записів.
5. Створення облікових записів для нових систем, які потрібні користувачеві. З часом можуть з'являтися нові системи або інструменти, до яких користувачеві потрібен доступ. На цьому етапі для нього створюються відповідні облікові записи.
6. Аудитору потрібен доказ того, хто до чого має доступ. Регулярно або за потреби проводиться аудит доступів. Система повинна надавати інформацію про те, які користувачі мають доступ до яких ресурсів, для забезпечення відповідності політикам безпеки та нормативним вимогам.
7. Користувач залишає організацію. Коли співробітник звільняється або з інших причин залишає компанію.

8. Система деактивує всі облікові записи користувача. Після виходу користувача з організації всі його облікові записи в усіх системах мають бути негайно деактивовані або видалені для запобігання несанкціонованому доступу.

Цей циклічний процес ілюструє постійне управління ідентифікаційними даними та доступами протягом усього часу перебування користувача в організації, враховуючи всі неминучі зміни, що відбуваються між цими двома подіями (приєднання та вихід).

2.3. Функції та можливості сховища платформи Delinea PAM

Secret Server — це комплексне рішення для керування привілейованим доступом (PAM), розроблене для захисту, контролю та управління привілейованими обліковими записами та обліковими даними в організації. Це рішення пропонує безпечне централізоване сховище для зберігання конфіденційної інформації, такої як паролі, ключі та сертифікати, водночас гарантуючи, що доступ до цих критично важливих активів надається лише уповноваженому персоналу [6-8].

Secret Server має розширені функції, такі як контроль доступу, аудит та автоматична ротація паролів. Secret Server дозволяє організаціям підтримувати надійний рівень безпеки, знижувати ризик витоку даних та дотримуватися нормативних вимог [6, 7].

До ключових функцій секретного сервера Delinea відноситься наступне [8-9]:

Безпечне зберігання паролів. Секретний сервер зберігає привілейовані облікові дані в зашифрованому форматі, захищаючи конфіденційну інформацію від несанкціонованого доступу [8-9].

Контроль доступу. Secret Server реалізує контроль доступу на основі ролей, що дозволяє адміністраторам встановлювати дозволи та контролювати, хто має доступ до конфіденційної інформації [8-9].

Керування ескалацією привілеїв. Secret Server інтегрується з системами Windows для забезпечення керування ескалацією привілеїв, допомагаючи зменшити ризик витоку даних [8-9]..

Аудит та звітність. Secret Server надає детальні журнали аудиту та звіти, що полегшує організаціям відстеження доступу до конфіденційної інформації та виявлення будь-якої несанкціонованої діяльності [8-9].

Автоматизоване керування паролями. Secret Server підтримує автоматизоване керування паролями, що допомагає оптимізувати процес керування паролями та зменшити ризик помилок, внесених вручну [8-9]..

Багатофакторна автентифікація. Secret Server підтримує багатофакторну автентифікацію, що допомагає покращити безпеку конфіденційної інформації [8-9]..

Інтеграція з іншими інструментами. Secret Server інтегрується з різноманітними іншими інструментами, включаючи Active Directory, Microsoft Azure та хмарні додатки, що спрощує для організацій керування паролями та засобами контролю доступу [8-9]..

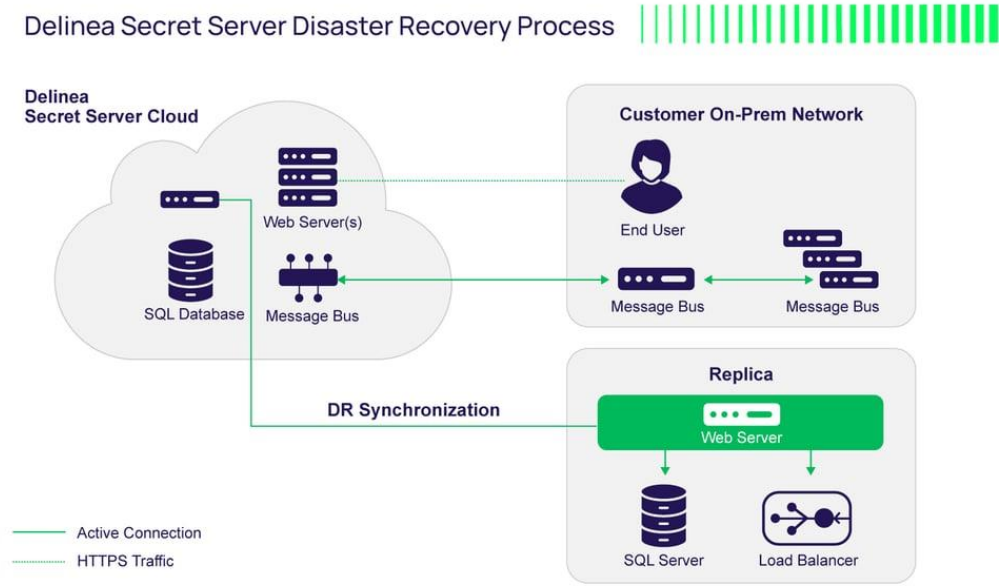

Рис. 2.3. Складові Secret Server

Розглянемо детально основні функції зберігання паролів, як це показано на рис.2.4.

1. Для забезпечення безпечного зберігання паролів Secret Server використовує 256-бітове шифрування AES є найсильнішим шифруванням, доступним для програмного забезпечення для керування паролями підприємств, і забезпечує неперевершену безпеку [8-9].

Рис.2.4. Функції зберігання паролів

Окрім шифрування секретних даних у стані спокою, Secret Server також можна використовувати з прозорим шифруванням даних (TDE) SQL Server для подальшого захисту даних. SSL/TLS можна застосовувати до всіх з’єднань для забезпечення наскрізного шифрування [9].

Secret Server генерує унікальний ключ шифрування під час встановлення. Цей ключ шифрується та зберігається у файлі encryption.config або керується HSM. Поєднання цього файлу та бази даних вашого Secret Server дозволяє відновити систему в будь-який момент.

Секретний сервер хешує та перетворює паролі локальних користувачів за допомогою випадково згенерованих алгоритмів хешування PBKDF2-HMAC-SHA256. Користувачі для входу в Active Directory автентифікуються безпосередньо в домені, а їхні паролі не зберігаються в базі даних Секретного сервера [9].

2. Для посилення безпеки доступу до секретного серверу використовується багатофакторна автентифікація — це метод автентифікації, що базується на чомусь відомому вам (пароль) і чомусь, що у вас є (одноразовий токен/PIN-код, тощо). Це гарантує, що навіть якщо пароль буде викрадено, зловмисник не зможе використати його для доступу до секретного сервера. Він також сприяє швидкому відновленню облікового запису [9].

Для цього можна використовувати різноманітні рішення для багатофакторної автентифікації, включаючи вже існуючу інфраструктуру автентифікації, для автентифікації користувачів перед наданням їм доступу до Secret Server.

Як приклад, Duo Security підтримує push-сповіщення безпосередньо на телефон користувача та апаратні токени, такі як YubiKey. Якщо додаток або токен користувача недоступні, також можна отримати телефонний дзвінок або текстове повідомлення для позасмугової автентифікації.

Інший метод, який можна застосувати -це Google Authenticator або будь-який додаток із програмними токенами, що підтримує TOTP (Microsoft Authenticator, Duo, Amazon MFA). Програмні токени – це безкоштовний та швидкий спосіб підвищити безпеку процесу входу, якщо немає комерційного багатофакторного рішення.

Secret Server підтримує будь-якого багатофакторного постачальника, який надає інтерфейс RADIUS, галузевий стандарт реалізації, що підтримується більшістю багатофакторних постачальників.

Багатофакторна автентифікація (MFA) для окремих секретних даних додає рівень безпеки до облікових даних із високим рівнем привілеїв. Ви можете застосувати багатофакторну автентифікацію до окремих облікових даних, щоб забезпечити захищений доступ на кожному рівні, водночас дозволяючи адміністраторам встановлювати стратегічний час проходження, щоб команди були продуктивними та продуктивними.

3. Функція обмеження IP-адрес надає можливість контролювати розташування та мережі, з яких користувачі можуть отримати доступ, налаштувавши Secret Server таким чином, щоб він був доступним лише для IP-адрес у певному діапазоні. Це дозволяє обмежити доступ до Secret Server користувачами, які перебувають «в мережі» та не підключаються через VPN тощо [9].

Функції керування секретним сервером допомагають швидко розпочати роботу та легко масштабуватися, додаючи більше систем, користувачів і секретів.

4. Функція створення папок та дозволів використовується у міру зростання вашої організації та додавання секретів до сховища, о потребує саме створення структура папок Secret Server допоможе вам залишатися організованими. Завдяки папкам кілька команд можуть використовувати центральне сховище, маючи доступ лише до тих областей, які їм призначені [9].

Не існує універсального рішення щодо того, як упорядкувати ваші привілейовані паролі. Налаштовувана структура папок Secret Server дозволяє налаштувати елементи керування доступом відповідно до потреб організації. Наприклад, ви можете упорядковувати папки на основі [9]:

– клієнти;
– географічні розташування;
– бізнес-одиниці;
– різні IT-команди, такі як адміністратори баз даних, адміністратори Unix та адміністратори Windows Server.

Можна вкладати папки на кількох рівнях, щоб керувати ними за допомогою структури, яка найкраще підходить.

Дозволи можна призначати для папок, підпапок і секретів. Наприклад, кожному користувачеві можна призначити особисту папку за замовчуванням, де він може зберігати часто використовувані паролі, такі як логіни для сайтів підтримки, ключі API для розробників або призначені ліцензії на продукти [9].

5. IT-відділи повинні захищати конфіденційні файли, такі як мережеві схеми, файли ліцензій та SSL-сертифікати, забезпечуючи при цьому легкий доступ до них для потрібних користувачів. Завдяки функції вкладених файлів Secret Server ви можете завантажувати конфіденційні файли, які будуть зашифровані та збережені разом з іншими привілейованими обліковими записами. RBAC та дозволи означають, що ви маєте детальний контроль над тим, хто може завантажувати та переглядати вкладені файли [9].

6. Багато організацій значно інвестують в Active Directory, щоб забезпечити користувачам єдину ідентифікаційну інформацію в організації. Використання існуючих груп та імен для входу в Active Directory допомагає швидко розгорнути Secret Server, зменшити накладні витрати на управління та покращити його впровадження [9].

Інтеграція з Active Directory надає адміністраторам простий та ефективний спосіб автоматичного надання та скасування доступу до Secret Server за допомогою вже існуючих інструментів та політик. Призначаючи доступ на основі груп безпеки, не доведеться вручну надавати дозволи щоразу, коли новому адміністратору потрібен доступ. Надаючи права на основі груп безпеки домену, можна гарантувати, що коли користувачі змінюють ролі, їхні права на Secret Server також змінюватимуться відповідно [9].

Інтеграція з Active Directory дозволяє користувачам входити за допомогою свого звичайного облікового запису домену, щоб отримати доступ до привілейованих облікових записів, таких як їхні облікові дані адміністратора домену [9].

Microsoft також надає додаткові параметри єдиного входу (SSO) та безпеки, які може використовувати Secret Server. За допомогою інтегрованої автентифікації Windows або ADFS ви можете забезпечити SSO для Secret Server [9].

Можуть бути випадки, коли Active Directory неможливий через розподіл обов'язків, середовище під жорстким контролем або відсутність домену. У таких ситуаціях Secret Server має власне сховище користувачів і груп і можливості, а зміни членства в групах можна делегувати між командами, щоб обмежити накладні витрати [9].

2.4. Функції запису сеансів на платформі Delinea

Delinea пропонує *базові або розширені* опції запису сеансів, яке забезпечується різними інструментами та конфігураціями, що дозволяють захоплювати контент різного рівня [10-11].

Базовий запис сеансів підтримує реєстрацію метаданих натискань клавіш для сеансів RDP та SSH без необхідності агента в середовищах Windows та Mac. Користувачі можуть натискати клавіші, а інтерфейс відтворення сеансів відображає цю додаткову інформацію про активність [10].

Розширений запис сеансів пропонує детальніші можливості та метадані обробки [10].

На платформі запису сеансів визначено інструменти записують відео:

– Обробник протоколу;
– Обробник протоколу на сервері з'єднувача сеансів;
– Заповнювач веб-паролів;
– ASRA (Агент розширеного запису сеансів);
– Привілейований віддалений доступ.

Для запису натискання клавіш використовуються наступні інструменти:

– RDP-проксі;
– SSH-проксі;

– ASRA (Агент розширеного запису сеансів);

– Обробник протоколу на сервері з'єднувача сеансів;

Наступні інструменти можуть записувати метадані процесу:

– ASRA (Агент розширеного запису сеансів).

Базовий запис сеансу – це ліцензована функція в Secret Server . Вона спирається на обробник протоколу, налаштований на клієнтських машинах через панель запуску Secret Server . За допомогою панелі запуску Secret Server робить скріншоти на клієнтській машині щосекунди під час записаного сеансу користувача. Ці зображення екрана користувача компілюються у відео, яке можна завантажити та відтворити для цілей аудиту та безпеки. Активність, записана під час сеансу, базується лише на змінах екрана. Це дійсно для панелей запуску Mac. Панели запуску RDP/SSH завантажують записані відеосегменти щосекунди.

З'єднувач сеансів секретного сервера використовує модифікований обробник протоколу, який підтримує запис натискань клавіш [10].

Моніторинг сеансів дозволяє адміністраторам з дозволом на моніторинг сеансів переглядати всі активні запущені сеанси на секретному сервері . Якщо запис сеансів увімкнено на секретному сервері, адміністратор може переглядати сеанс користувача в режимі реального часу [11].

Адміністратори можуть шукати серед активних та завершених сеансів. Щоб переглянути та здійснити пошук серед сеансів, перейдіть до розділу Адміністратор > Моніторинг сеансів [10].

Пошук по сесіях може містити різні дані. Щоб вибрати, які дані шукати, необхідно налаштувати параметри фільтрів пошуку.

Деякі фільтри пошуку вимагають встановлення або налаштування додаткових компонентів:

Дані клієнта проксі-сеансу : Пошук у даних натискань клавіш проксі-сеансів SSH. Потрібно, щоб проксі-сервер SSH був увімкнений, і сеанси SSH використовували його.

Дані натискання клавіш RDP: Потрібно, щоб на цільовому пристрої було встановлено ASRA, або щоб були доступні компоненти проксі-сервера RDP чи з’єднувача сеансу.

Ім'я застосунку RDP: Потрібно встановити додатковий ASRA на цільовому пристрої.

Розглянемо процедуру запису сенсу користувача, який підключається до секретного сервера.

Користувач підключається до SS та натискає кнопку запуску секретного ключа з не проксі-сеансом. Це налаштування за замовчуванням. Запис сеансу ввімкнено для секретного ключа. Цей сценарій стосується як SS, так і SSC (рис.2.5) [10-11].

Спрощений потік: Користувач > SS > Запуск протоколу > Кінцева точка системи.

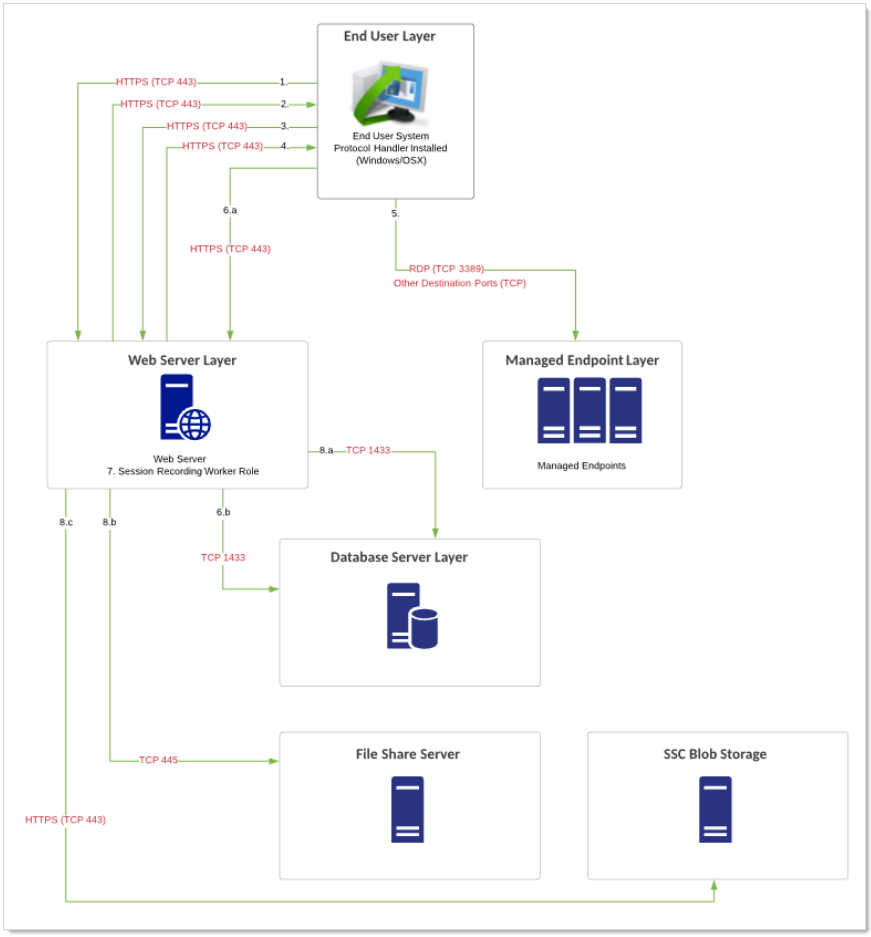

Рис.2.5. Процедура підключення користувача до секретного сервера

1. Користувач входить до SS. Користувач натискає значок, щоб розпочати сеанс для секретного ключа в SS з увімкненим записом сеансу.

2. SS запускає обробник протоколу.

3. Обробник протоколу запитує інструкції від SS.

4. SS надсилає секретний код та цільовий віддалений сервер.

5. Засіб запуску протоколу запускає сеанс RDP з цільовим сервером. Починається запис.

6. Система кінцевого користувача через обробник протоколу виконує одну з двох речей:

7. RDP/SSH лаунчери: Завантажує записані відеосегменти щосекунди.

– Програми запуску Mac: Робить скріншоти щосекунди. Ця інформація завантажується через HTTPS (налаштовується) та зберігається в базі даних.

– Роль запису сеансів веб-серверів виконує будь-яке кодування, перекодування або перекомпозицію відео, щоб забезпечити їх відтворення через сторінку моніторингу сеансів.

8. Остаточний відеозапис зберігається в базі даних або на сервері спільного доступу до файлів (бажано) після обробки відео. Для клієнтів Secret Server Cloud він зберігається у специфічному для клієнта BLOB-об'єкті. Відтворення можливе лише через розділ «Моніторинг сеансів» у SS.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1. Варіант створення облікових записів на платформі Delinea

Розглянемр порядок керування користувачами на платформі Delinea. Для цього на головному екрані необхідно обрати «Доступ» у лівому меню навігації, а потім виберіть «Користувачі» . На сторінці «Користувачі» відображаються всі користувачі платформи, включаючи користувачів Active Directory та користувачів Delinea Directory (локальних) (рис 3.1).

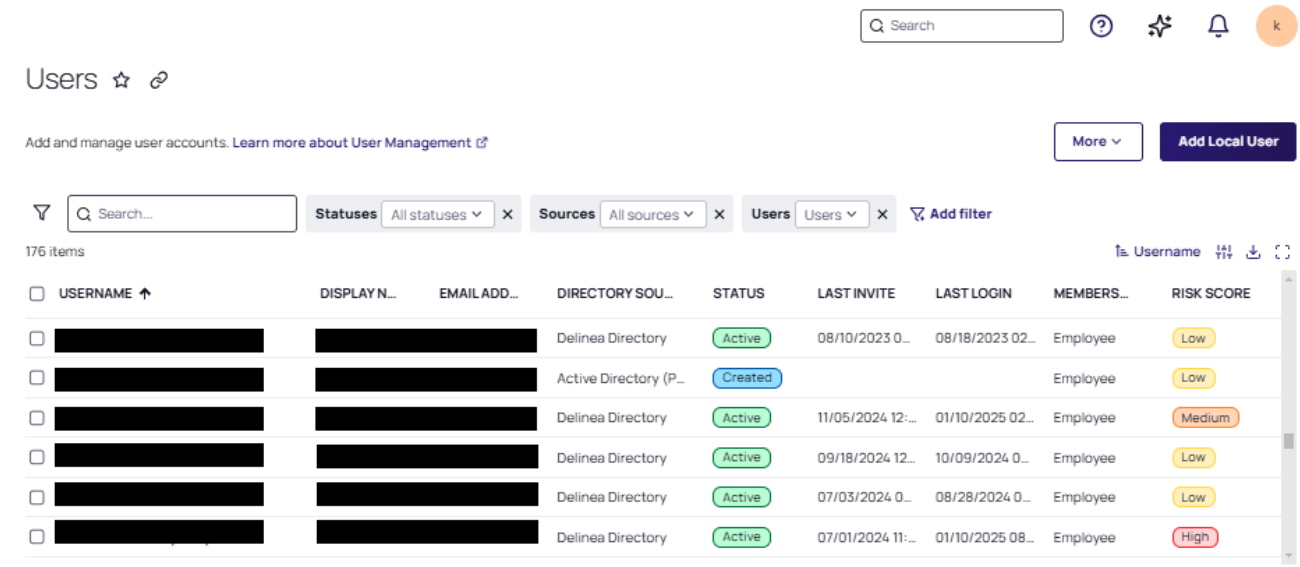

Рис. 2.1. Сторінка користувачів на платформі Delinea

Клацнувши *ІМ'Я КОРИСТУВАЧА* можна перейти на сторінку цього конкретного користувача, де можна переглядати та редагувати налаштування облікового запису користувача, включаючи членство в групах, ролі, політики, дії та атрибути користувача.

Оцінка ризику відображається для кожного користувача. Ризик базується на аналітиці, яка генерує невирішені сповіщення, та пов'язаних з ними результатах. Оцінки ризику призначаються як низький , середній та високий [13], як це показано у таблиці 3.1.

Таблиця 3.1.

Оцінка ризиків роботи користувачів

Рівень ризику	**Визначення**
Немає даних	Для цього користувача не виявлено жодного ризику. Системи моніторингу не виявили жодної підозрілої поведінки чи проблем безпеки.
Низький	Для цього користувача було спрацювало незначне сповіщення безпеки. Зазвичай ці сповіщення не викликають занепокоєння та можуть бути результатом законних дій, таких як доступ до ресурсів із незвичного географічного розташування. Негайних дій не потрібно, але рекомендується продовжувати моніторинг.
Середній	У цього користувача спостерігаються підвищені показники ризику. Це може включати численні сповіщення або моделі поведінки, які вимагають подальшого розслідування. Хоча ситуація не є критичною, рекомендується вжити проактивних заходів, таких як посилений моніторинг або перевірка активності користувача.
Високий	Для цього користувача виявлено значні показники ризику. Приклади включають: Кілька підозрілих дій в обліковому записі Спроба бомбардування MFA (багатофакторної автентифікації) з подальшою аномальною активністю У ситуаціях високого ризику наполегливо рекомендуються такі дії: Застосуйте для користувача безпечніший метод багатофакторної автентифікації (наприклад, апаратні токени або автентифікацію на основі додатків). Співпрацюйте з користувачем для виявлення та зменшення потенційних ризиків.

	Вживайте негайних заходів, щоб запобігти спробам захоплення облікового запису.

Оцінку ризиків генеруються на основі Аналітики, після чого створюються сповіщення на основі різних правил, відхилення від цих правил або будь-якого виявленого ризику в обліковому записі. Наприклад, сповіщення може бути згенероване, коли робиться спроба вгадати пароль облікового запису.

На основі сповіщень, що спрацьовують для кожного користувача, платформа Delinea розраховує ризик облікового запису платформи. Цей ризик враховується лише тоді, коли сповіщення не вирішено. Функція аналітики розраховує оцінку ризику для кожного користувача: низький, середній, високий або «Н/Д», якщо для користувача не знайдено жодних сповіщень.

У Центрі загроз можна керувати сповіщеннями та колекціями сповіщень, які називаються випадками, щоб швидко виявляти загрозливі дії та оперативно реагувати на кожну проблему.

Практично кожен обліковий запис користувача на платформі має бути *зовнішнім обліковим* записом користувача, тобто або обліковим записом Active Directory, або федеративним обліковим записом.

Локальний обліковий запис користувача додається безпосередньо до платформи адміністратором.

Зовнішній обліковий запис користувача не додається безпосередньо до платформи, але стає доступним на платформі, коли пов’язаний Active Directory або федерація підключається до платформи.

Адміністратор все одно повинен надати користувачеві дозволи на доступ до функцій платформи.

Локальний користувач повинен відповідати вимогам локальної автентифікації для входу на платформу.

Зовнішній користувач повинен відповідати вимогам автентифікації лише через зовнішнє джерело (AD або постачальник ідентифікаційних даних федерації).

Локальний обліковий запис користувача відображається на сторінці Користувачі (Доступ > Користувачі), коли адміністратор додає обліковий запис до платформи.

Зовнішній обліковий запис користувача відображається на сторінці Користувачі лише після першого входу користувача на платформу.

Для подальшої роботи адміністратору необхідно управляти обліковими записами користувачів тому розглянемо порядок як виконувати різні адміністративні завдання для управління обліковими записами користувачів на платформі Delinea. Основні дії адміна з користувачами платформи показано у таблиці 3.2.

Таблиця 3.2.

Основні дії адміністратора

Дія	**Опис**
Встановити пароль	Запропонує вам скинути пароль облікового запису користувача. У вікні, що з’явиться, введіть новий пароль для користувача.
Надіслати запрошення електронною поштою	Надсилає електронний лист вибраному користувачеві. У рамках цього робочого процесу користувач повинен змінити свій пароль під час наступного входу в систему.
Розблокування MFA	Призупиняє багатофакторну автентифікацію на 10 хвилин. Багатофакторна автентифікація вимагає від користувачів виконання додаткових кроків, таких як підтвердження своєї особи електронною поштою або телефонним дзвінком, для входу на платформу Delinea. Якщо у користувача виникають проблеми зі входом, виберіть користувача та виберіть цю дію, щоб дозволити йому ввійти лише за допомогою імені користувача та пароля.
Вимкнути	Вимкнути обліковий запис користувача. Вимкнений

обліковий запис	користувач не може увійти на платформу. Якщо користувач наразі увійшов у систему, він не зможе отримати доступ до служб платформи, які потребують автентифікації.
Розблокувати обліковий запис	Коли обліковий запис користувача блокується тимчасово або назавжди, що зазвичай відбувається через певні політики або умови, ця дія дозволяє адміністратору негайно розблокувати обліковий запис. Ця дія доступна лише тоді, коли заблоковано локальний обліковий запис користувача.
Права на поповнення	Дозволяє негайно перезавантажувати кешовані ідентифікаційні дані користувача з його служби каталогів, усуваючи необхідність очікування синхронізації. Ця дія особливо корисна, коли дані користувача було оновлено у віддаленій службі каталогів, але ще не відображено на платформі.

Платформа дозволяє детально розглянути інформацію про окремого користувача за замовчуванням відкривається на вкладці «*Огляд*».

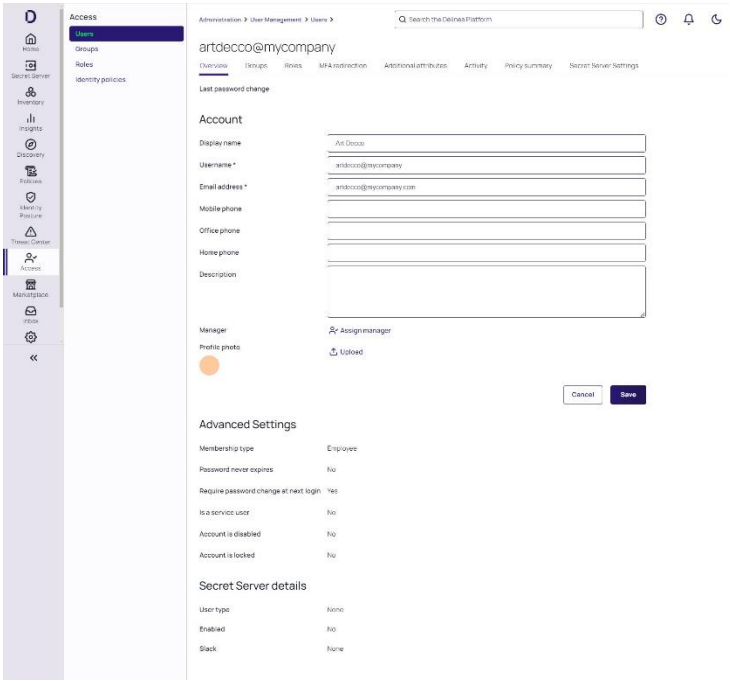

Рис. 3.1. Сторінка «Огляд»

У верхній частині вкладки «Огляд» відображається основна інформація про обліковий запис користувача, включаючи стан, джерело каталогу, дату створення, останній вхід та останню зміну пароля.

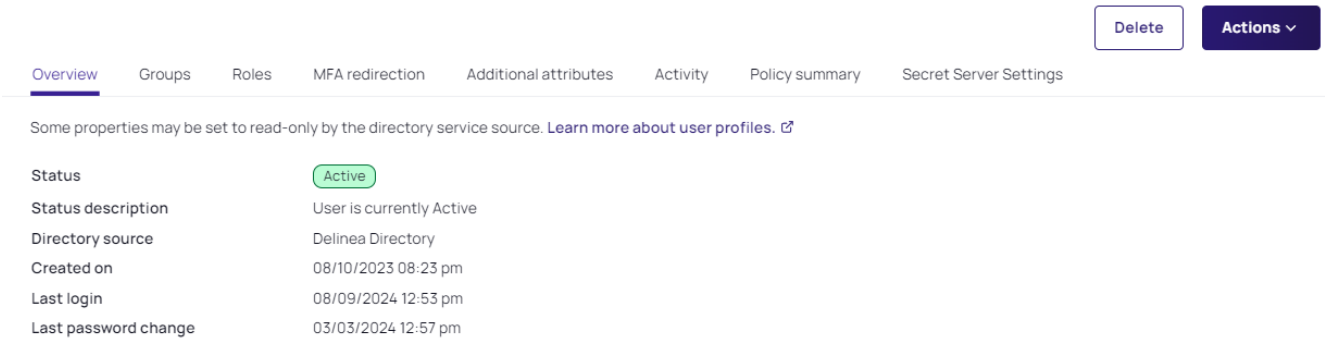

Рис. 3.2. Основна інформація про обліковий запис користувача

До кожного користувача може застосовуватись опис статусу, як це показано в наступній таблиці 3.3.

Таблиця 3.3.

Опис статусу користувача

Статус	**Опис**
Активний	Користувач увійшов на платформу Delinea.
Запрошено	Адміністратор надіслав запрошення користувачеві, але користувач ще не прийняв його та не увійшов у систему. Ви можете надіслати запрошення під час створення локального облікового запису або після створення користувача. Коли користувач прийме запрошення, йому буде запропоновано скинути пароль, перш ніж він зможе увійти на платформу.
Створено	Обліковий запис було створено на платформі, але запрошення електронною поштою не було надіслано. Успішно налаштовані користувачі відображаються на сторінці "Користувачі" зі статусом "Створено".
Призупинено	Обліковий запис користувача заблоковано. Існує кілька причин блокування облікового запису; наприклад, його може

	заблокувати системний адміністратор або користувач досяг максимальної кількості спроб входу. Користувачів може бути автоматично призупинено через кілька одночасних збоїв пароля. У такому випадку: Користувачі автоматично блокуються на 30 хвилин. Обліковий запис адміністратора за замовчуванням (cloudadmin@< tenant >) також може бути призупинено з тієї ж причини; проте автоматичне призупинення триває лише 5 хвилин. Якщо додаткові спроби входу будуть здійснені з неправильним паролем, час блокування буде подовжено. Автоматичне призупинення завершується після успішного входу користувача в систему. На вкладці **«Користувачі»** продовжуватиме відображатися статус «Призупинено», доки користувач успішно не ввійде в систему.

Обліковий запис

У розділі «Обліковий запис» натисніть «Редагувати» , щоб змінити поля атрибутів або завантажити зображення профілю (рис 3.3):

Відображуване ім'я : ім'я, яке бачать користувачі після входу на платформу.

Ім’я користувача : ім’я, яке використовується для входу на платформу. Користувачі входять за допомогою <Login Name>@<domain>. Наприклад, stepanov@duikt.com.

Рис. 3.3. Розділ «Обліковий запис»

Адміністратор може керувати членством у групах з окремого перегляду

користувачів, як описано тут, або з перегляду груп.

1. Натисніть вкладку Групи , щоб переглянути список груп, до яких належить користувач.

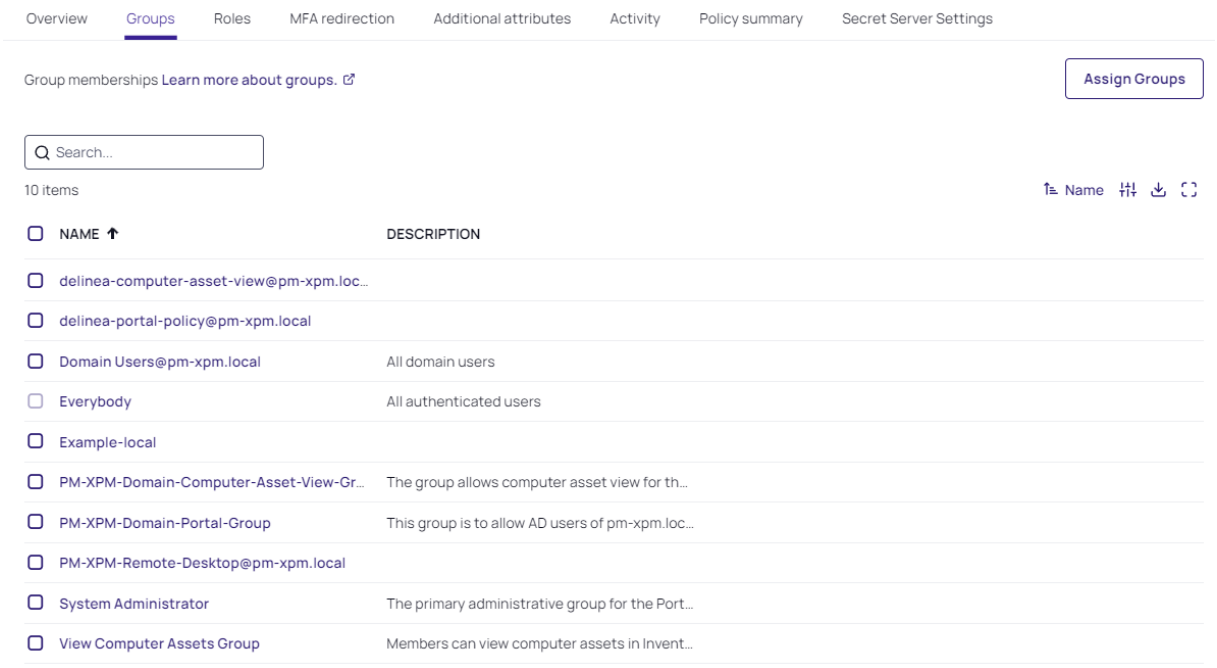

Рис.3.4. Список груп

2. Щоб додати користувача до групи, натисніть «Призначити групи» .

3. Виберіть одну або декілька груп.

4. Натисніть кнопку «Додати» , щоб додати користувача до вибраних груп.

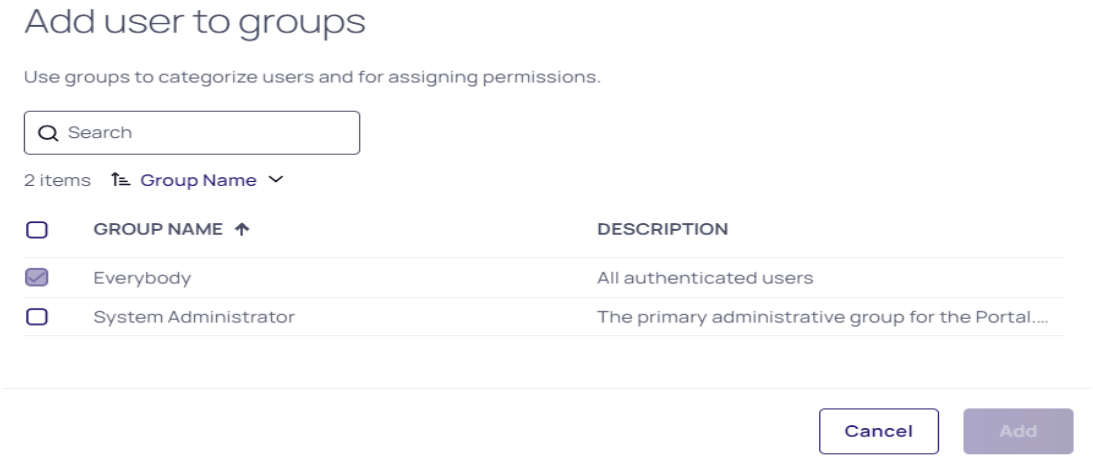

Рис.3.5. Додавання користувача до групи

5. Щоб видалити користувача з групи, наведіть курсор на рядок групи, ближче до правого кінця стовпця « Ім’я» , і натисніть значок кошика, що з’явиться.

Вкладка перенаправлення MFA

Перенаправлення багатофакторної автентифікації (MFA) дозволяє користувачам виконувати MFA від імені будь-якого обраного користувача. Це означає, що користувача, який входить у систему, можна налаштувати на виконання MFA як користувача перенаправлення та отримати токен ідентифікації для початкового користувача, який увійшов, після успішного входу. Після налаштування перенаправлення MFA обробляється автоматично.

Щоб пояснити, як працює перенаправлення, розглянемо двох наступних користувачів:

Початковий користувач входу. Користувач, який активно намагається увійти.

Перенаправлений користувач. Користувач, у якого налаштовано багатофакторну автентифікацію (MFA). Спроби входу перенаправляються цьому користувачеві для відповіді на будь-які запити MFA.

Користувач, що перенаправляє, виконує багатофакторну автентифікацію (MFA) від імені користувача, який спочатку ввійшов у систему. Будь-який механізм MFA, що використовується, такий як електронна пошта, текстове повідомлення, мобільний автентифікатор тощо, виконується користувачем, що перенаправляє. Процедура виглядає наступним чином:

1. Початковий користувач намагається увійти, використовуючи своє ім'я користувача.

2. Дані оригінального користувача, який ввійшов у систему, отримані з платформи Delinea .

3. Перенаправлений користувач отримує виклики MFA для облікового запису перенаправленого користувача.

4. Після успішної автентифікації користувачеві, який ввійшов у систему, надається токен/файл cookie ідентифікації.

Типові випадки використання перенаправлення MFA

Перенаправлення MFA зазвичай використовується, коли у вихідного

користувача не налаштовано жодних атрибутів, і тому він не може задовольнити жодні MFA-запиті. Коли вихідному користувачеві надсилається запит на додаткову автентифікацію, функцію MFA-перенаправлення можна налаштувати таким чином, щоб використовувати MFA-запиті перенаправленого користувача (у якого налаштовано необхідні механізми).

Налаштування перенаправлення MFA

1. Перейдіть на вкладку Перенаправлення MFA . На цій вкладці вказано, чи ввімкнено перенаправлення MFA, і якщо так, то ім’я облікового запису перенаправлення.

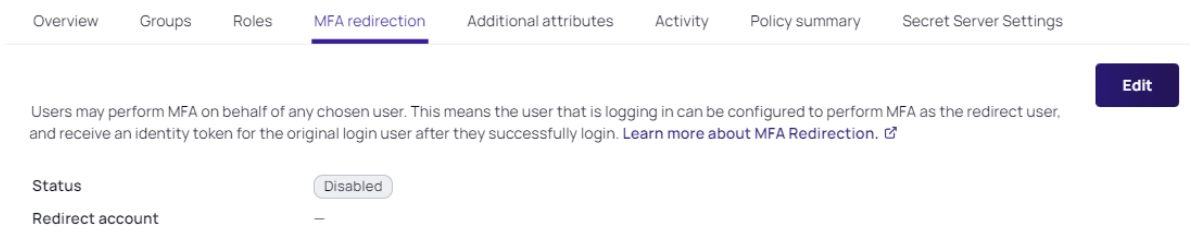

Рис.3.5. Вкладка перенаправлення MFA

2. Натисніть «Редагувати» .

3. Установіть прапорець «Увімкнути перенаправлення багатофакторної автентифікації на інший обліковий запис користувача».

Натисніть кнопку «Вибрати» та виберіть обліковий запис, який потрібно використовувати для перенаправлення MFA.

Вкладка «Активність»

На вкладці «Активність» перелічено кожну активність (подію) користувача на платформі, зокрема наступне:

– Вхід
– Вийти
– Набір секретних питань
– Зміна пароля
– Не вдалося змінити пароль
– Зміна пароля AD

– Не вдалося змінити пароль AD

Для кожної дії відображається така інформація:

– Дата/час

– Назва події

– Статус (Успіх або Невдача)

– Браузер

– IP-адреса

– Операційна система

Вкладка «Підсумок політики»

На вкладці «Підсумок політик» відображається вся інформація про існуючі політики, пов’язані з певним користувачем. Сторінка не надає можливості редагування, оскільки всі ці політики керуються в іншому місці.

Рис. 3.6. Вкладка «Підсумок політики»

Вкладка налаштувань секретного сервера

На вкладці «Налаштування секретного сервера» відображаються налаштування користувача для секретного сервера.

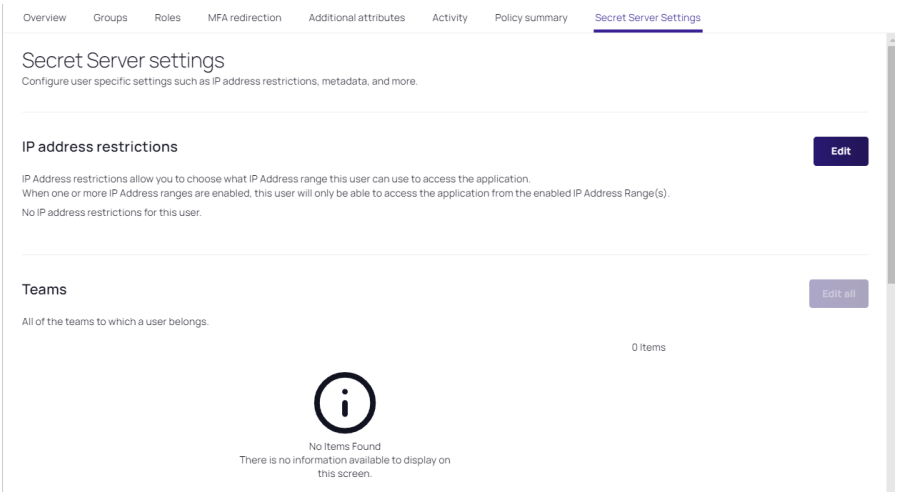

Рис.3.7. Налаштування секретного сервера

Правильно створенні користувачі привілейованих записів організації, дозволять управляти їх доступом до інформаційної системи організації та своєчасного виявлення ризиків безпеки та захисту інформаційної системи організації від несанкціонованого доступу.

3.2. Розробка рекомендацій щодо використання рішень управління привілейованим доступом в організаціях

Управління привілейованим доступом на сьогодні є критично важливим компонентом стратегії кібербезпеки будь-якої організації. Такі рішення допомагають організаціям проводити постійний контроль та моніторинг доступу до критичних систем та даних інформаційної системи організації, мінімізуючи ризики, пов'язані з несанкціонованим використанням привілейованих облікових записів.

1. До основних принципів впровадження PAM є застосування принципи найменших привілеїв. Це полягає в надані користувачам, додаткам та системам лише ті мінімально необхідні права доступу, які потрібні для виконання їх безпосередніх завдань. Регулярний перегляд та відкликання зайвих привілеїв підвищують безпеку привілейованих облікових записів.

Саме впровадження моделі нульової довіри (Zero Trust), яка полягає у «Не довіряйте нікому за замовчуванням», незалежно від того, чи знаходиться користувач всередині чи поза корпоративною мережею. Необхідно постійно перевіряти кожен запит на доступ, автентифікувати та авторизувати користувачів перед наданням доступу до ресурсів. Правильно сегментована мережа та система , розділить критичні системи з суворим контролем доступу між ними. Це допоможе обмежити потенційну шкоду в разі компрометації одного з сегментів.

2. Інвентаризація та управління обліковими записами шляхом визначення та створення каталогів дозволять правильно розподілити їх по групах. Сюди входять облікові записи адміністраторів систем, баз даних, мережевого обладнання, сервісні облікові записи, облікові записи додатків, а також облікові записи сторонніх постачальників. Такий підхід забезпечить надійне зберігання та ротацію паролів для паролів привілейованих облікових записів. Для кожного облікового запису необхідно впровадити політики регулярної та автоматичної зміни паролів, а також використання складних та унікальних паролів. Кожен привілейований користувач повинен мати унікальний обліковий запис для забезпечення підзвітності та відстеження дій.

3. Впровадження на багатофакторну автентифікацію (MFA) значно підвищує рівень захисту, навіть якщо пароль буде скомпрометовано. Необхідно надавати привілейований доступ лише на обмежений період часу, необхідний для виконання конкретного завдання. Після завершення завдання доступ автоматично відкликається.

4. Контролювати доступ на основі ролей (Role-Based Access Control, RBAC) за рахунок визначення ролей на основі функціональних обов'язків та надавати привілеї відповідно до цих ролей.

5. Моніторинг, аудит та реагування. Необхідно записувати та проводити моніторинг всіх сеансів привілейованого доступу: Це дозволить виявляти підозрілу активність, розслідувати інциденти безпеки та забезпечувати відповідність нормативним вимогам. Крім цього необхідно проводити аудит привілейованого

доступу, шляхом перегляду журналів активності, прав доступу та конфігурації PAM-системи для виявлення аномалій та потенційних вразливостей.

6. Розроблювати та впроваджувати процедури реагування на інциденти для того щоб мати чіткий план дій на випадок компрометації привілейованого облікового запису або іншого інциденту безпеки, пов'язаного з PAM.

7. Автоматизуйте процеси безпеки пов'язані з управлінням привілейованим доступом, такі як ротація паролів, моніторинг та сповіщення про підозрілу активність.

8. Організаційні аспекти полягають у наступному що успішне впровадження PAM-рішення вимагає підтримки та розуміння важливості цього процесу з боку вищого керівництва. Навчання персоналу полягає у регулярному проведенні тренінгів для всіх користувачів, які мають привілейований доступ, щодо політик безпеки, правильного використання PAM-системи та розпізнавання потенційних загроз.

9. Розробка та документування політик та процедур створить чіткі та зрозумілі політики щодо управління привілейованим доступом та відповідні процедури їх виконання.

10. Регулярне оновлення та тестування PAM-рішень дозволять впевнитися, що ваше PAM-рішення оновлюється до останньої версії та відповідають функціональності та ефективності.

11. Інтеграція з іншими системами безпеки, такими як SIEM (Security Information and Event Management), IDM (Identity Management) та іншими, для створення комплексного підходу до захисту підвищують безпеку привілейованих записів організації.

Отже, впровадження та ефективне використання PAM-рішень є безперервним процесом, який вимагає постійної уваги, аналізу та вдосконалення. Дотримання цих рекомендацій допоможе організаціям значно знизити ризики, пов'язані з привілейованим доступом, та посилити загальний рівень кібербезпеки.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проаналізовано проблему ідентифікації користувачів інформаційної системи організації, який показав необхідність використовувати методи та засоби управління привілейованими користувачам, з метою збільшення рівня захисту привілеїв для зменшення несанкціонованому витоку інформації через скомпрометовані облікові записи.

Проведений порівняльний аналіз, відповідно до стратегії впровадження PAM, різних рішень управління привілейованим доступом показав, що Delinea PAM виділяється своїм фокусом на простоті та зручності використання, особливо для організацій, які активно переходять у хмару або вже мають гібридну інфраструктуру. Їх хмарно-орієнтована архітектура забезпечує легке розгортання, масштабування та інтеграцію з сучасними інструментами та сервісами.

В роботі показано, що архітектура платформи Delinea PAM є динамічною, яка керується штучним інтелектом та заснована на ризиках. Функціональний опис основних компонентів платформи надає чітке уявлення щодо життєвого циклу привілеїв у системі, їх зберігання на секретному сервері та моніторингу сесій.

В роботі запропоновано варіант налаштування користувачів привілейованого доступу, в основу якого закладено рольову модель доступу. Таке налаштування дозволить фахівцям з кібербезпеки краще надавати відповідні дозволи згідно політик безпеки організації для швидкого реагування та виявлення інцидентів.

В результаті виконання роботи надано рекомендації щодо використання платформи Delinea PAM щодо застосування методів та засобів привілейованого доступу.

Таким чином реалізація таких методів та засобів привілейованого доступу інформаційної системи організації повинна сприяти розвитку та ефективному захисту інформаційної системи організації від витоку інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cost of a data breach 2024/IBM URL: https://www.ibm.com/reports/data-breach .
2. Стратегія PAM. URL: https://www.linkedin.com/pulse/comprehensive-guide-developing-effective-pam-privileged/.
3. Форбс URL: https://www.forbes.com/sites/chuckbrooks/2025/03/05/cybersecurity-trends–statistics-for-2025-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/
4. Життєвий цикл облікового запису. URL: https://docs.delinea.com/online-help/account-lifecycle-manager/start.htm .
5. Управління життєвим циклом ідентифікації. URL: https://docs.delinea.com/online-help/delinea-platform/iga/identity-lifecycle-management-overview.htm .
6. Секретний сервер. URL: https://docs.delinea.com/online-help/delinea-platform/using-secrets/index.htm .
7. Функції Secret Server. URL: https://docs.delinea.com/online-help/secret-server/start.htm.
8. Основні завдання секретного сервера. URL: https://delinea.com/blog/secret-server-release-increases-resiliency-and-security.
9. Secure vault and password manager. URL: https://delinea.com/products/secret-server/features/secure-vault-and-password-manager.
10. Запис сеансів. URL: https://docs.delinea.com/online-help/secret-server/session-recording/session-rec-overview.htm .
11. https://docs.delinea.com/online-help/architecture/secret-server/session-recording-architecture/index.htm .
12. Arcon. URL: https://arconnet.com/privileged-access-management/ .
13. Користувачі Delinea. URL: https://docs.delinea.com/online-help/delinea-platform/users/index.htm .

14. BeyondTrust. URL: https://goteleport.com/use-cases/privileged-access-management/ .
15. CyberArk. URL: https://www.cyberark.com/.
16. Гайдур Г. І., Гахов С. О., Дмітрієв В. Є., Ганченко М. І. Актуальність та перспектива розвитку Privileged Access Management рішень. Зв'язок.- № 1 (2022).- С. 3-9.
17. Delinea PAM. URL: https://delinea.com/ .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)