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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованим доступом інформаційної системи організації на базі рішення Delinea»

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

_____ Анатолій ЮХИМОВИЧ
(підпис)

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

Керівник д.т.н., професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PUM - управління привілейованими користувачами

PIM - управління привілейованою ідентифікацією

PAM - управління привілейованим доступом

PTA - привілейована аналітика загроз

ВСТУП

Актуальність дослідження. Управління привілейованим доступом (PAM) має вирішальне значення для організацій, щоб покращити кібербезпеку та захистити конфіденційні дані та критично важливі системи. Впровадження технології привілейованого доступу може зменшити внутрішні загрози в організаціях. Це може бути досягнення за рахунок обмеження доступу до конфіденційних систем і даних лише авторизованим особам. Це зменшує ризик навмисного чи ненавмисного зловживання працівниками або підрядниками своїми привілеями.

Технологія управління привілейованого доступу зменшує поверхню атаки зодо заовнішньої загрози. Зовнішні зловмисники часто націлюються на привілейовані облікові записи, оскільки вони забезпечують шлях до конфіденційної інформації та критичних систем організації. PAM допомагає захищати та контролювати ці облікові записи, що ускладнює компрометацію системи для зовнішніх загроз.

Сьогодні організації повинні відповідати вимогам закону, таким як Закон України «Про захист персональних даних», GDPR, та PCI DSS, які зобов’язують запровадити жорсткий контроль доступу та моніторинг. PAM допомагає організаціям відповідати цим вимогам відповідності, запроваджуючи найменш привілейований доступ і зберігаючи контрольний слід привілейованих дій.

Крім цього PAM використовує принцип найменших привілеїв, гарантуючи, що користувачі мають лише мінімальний рівень доступу, необхідний для виконання своїх робочих функцій. Це зменшує поверхню атаки та обмежує потенційний вплив інцидентів безпеки.

Рішення PAM надають надійні функції обліковими обліковими записами, такі як зберігання, ротація та розподіл привілейованих облікових записів. Це допомагає запобігти неавторизованому доступу через скомпрометовані або витік облікових записів.

Особливістю використання технології PAM є можливість відстежувати та записувати привілейовані сеанси в реальному часі. Це не тільки допомагає виявляти підозрілу діяльність, але й забезпечує виявлення кіберслідів для розслідування інцидентів безпеки.

Впровадження PAM зменшує ризик несанкціонованого доступу, зловживання привілеями та витоку даних. Контролюючи та відстежуючи привілейований доступ, організації можуть проактивно виявляти та усунути загрози безпеці до їх ескалації.

Таким чином, можна стверджувати що управління привілейованим доступом відіграє велике значення для підтримки надійної безпеки інформаційної системи організації, відповідності вимогам і захисту від широкого спектру внутрішніх і зовнішніх загроз. Тому тема кваліфікаційної роботи на освітній ступінь «Магістра» є актуальною.

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

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

Мета роботи – розробити варіант технології управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації щодо застосування рішення в інформаційній системі організації.

Наукові завдання:

- провести аналіз проблеми управління привілейованим доступом до інформаційної системи організації;
- проаналізувати основні загрози інформаційній системі організації;
- провести аналіз існуючих рішень щодо управління привілейованим доступом до інформаційної системи організації;
- проаналізувати методи та засоби управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea;

- розробити варіант схеми розгортання управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління привілейованим доступом до інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці технології управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації фахівцям з кібербезпеки щодо застосування технології в інформаційній системі організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЙ

1.1. Аналіз змісту поняття привілейованого доступу до інформаційної системи організації

Привілейований доступ допомагає організаціям керувати та захищати доступ до найважливіших систем, програм і даних, які зазвичай зарезервовані для привілейованих облікових записів. Привілейовані облікові записи мають підвищені дозволи та можливості, що дозволяє цим користувачам виконувати різні адміністративні завдання, отримувати доступ до конфіденційної інформації та вносити зміни, які звичайні користувачі не можуть.

PAM працює за допомогою поєднання людей, процесів і технологій, що дозволяє організаціям захистити свої критично важливі активи шляхом суворого контролю над тим, хто може отримати доступ до привілейованих облікових записів і як вони можуть ними користуватися. У результаті організації можуть мінімізувати ризик несанкціонованого доступу до конфіденційних систем і даних, забезпечивши надійний підхід до керування привілейованими обліковими записами та гарантуючи, що лише авторизовані особи можуть ними користуватися.

Користувачі з привілейованим доступом зазвичай є адміністратори системи, які несуть відповідальність за її конфігурацію, безпеку, резервне копіювання і нагляд. Вони можуть мати повний доступ до всіх ресурсів системи, включаючи файли, бази даних, мережеві налаштування тощо. Важливо зазначити, що доступ з привілеями повинен бути обмеженим і контрольованим. Це забезпечить безпеку інформаційної системи та запобігатиме можливості зловживання адміністративними привілеями. Для цього можуть застосовуватися методи аутентифікації та авторизації, а також ведення журналів дій користувачів з привілеями для виявлення ненормальної або небезпечної активності.

Сьогодні будь-яка компанія для своєї роботи має свою інфраструктуру на базі якої працює інформаційна система (рис 1.1). Таку архітектуру можна представити

у вигляді декілька рівнів. Для кожного рівня можуть бути різні користувачі. З визначених користувачів такої інфраструктури повинні бути користувачі, які є її адміністраторами і мають спеціальні права. Тобто у таких користувачів є вищі привілеї доступу, ніж у звичайного працівника компанії. Отже надалі спробуємо надати зміст поняття привілейованого доступу до інформаційної системи організації.

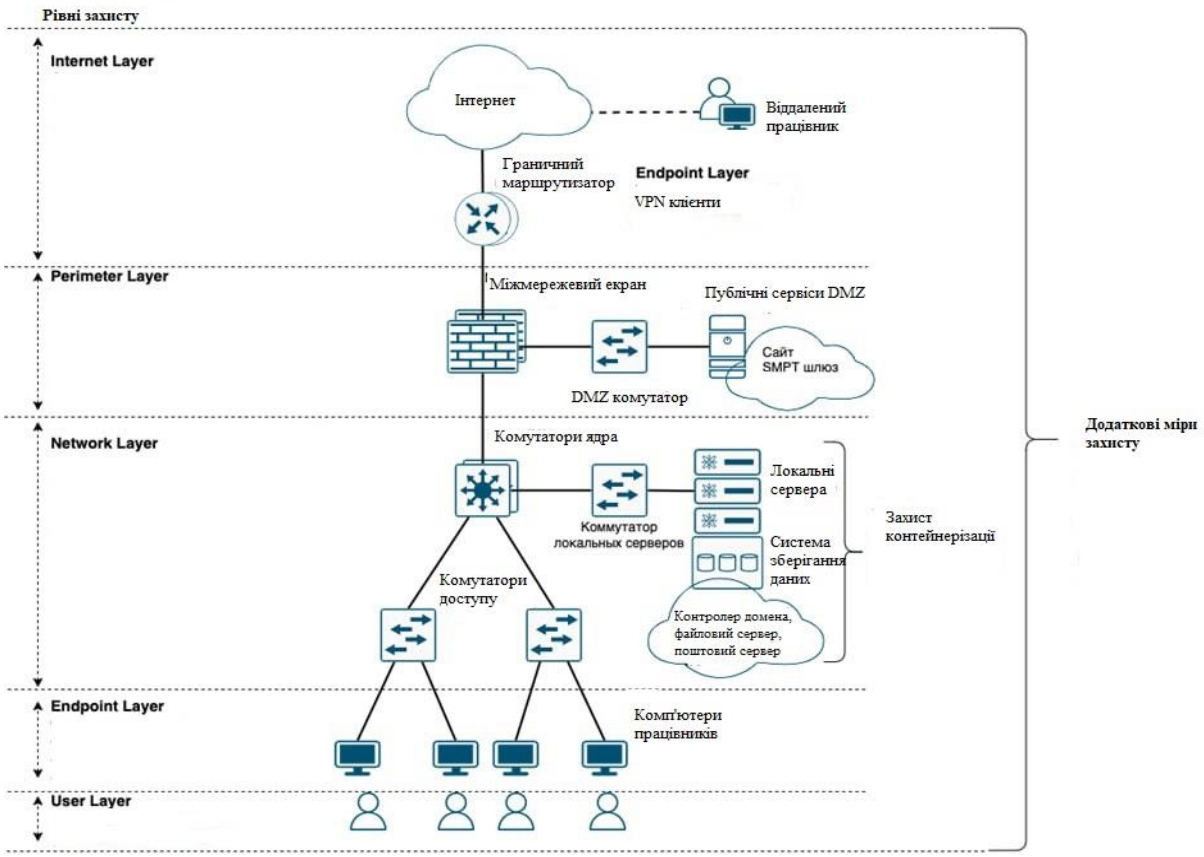

Рис.1.1. Архітектура інформаційної системи організації

Управління привілейованими користувачами, яке іноді називають PUM — це процес управління обліковими записами привілейованих користувачів, пов’язаних із певними активами. [1, 9]

Іноді PUM є синонімом управління привілейованою ідентифікацією (PIM). В обох випадках привілейований обліковий запис не пов’язано з конкретною особою, а скоріше є цифровою ідентифікацією, яку можна передати.

Привілейовані облікові записи покладаються на облікові дані для контролю доступу та поведінки. Створюючи та зберігаючи привілейовані облікові дані

(паролі, ключі та секрети) у безпечному сховищі та керуючи ними, рішення PAM контролюють авторизований доступ користувача, процесу чи систем до захищених ресурсів у IT-середовищі.[1]

PAM включає рішення для управління повним життєвим циклом усіх типів привілейованих облікових записів, від виявлення до надання та зміни, а також виведення з експлуатації. За допомогою PAM компанії можуть впроваджувати рівні доступу, включаючи затвердження, моніторинг сеансів та запис. Аналітика корпоративного рівня та реагування на інциденти, включені в комплексний PAM, дозволяють звітувати про відповідність аудиторам і керівникам, а також підтримувати спільну роботу команди IT і безпеки, щоб запобігти атакам на кібербезпеку привілеїв і реагувати на них.

Управління привілейованим доступом (PAM) містить інструменти контролю безпеки та керування політикою для управління та контролю доступу до привілейованих облікових записів, робочих станцій і серверів. Привілейовані облікові записи - це облікові записи з підвищеними дозволами, наприклад облікові записи адміністратора. PAM контролює, хто може використовувати ці облікові записи для виконання критично важливих завдань, таких як встановлення програмного забезпечення, внесення змін до налаштувань системи або доступ до конфіденційних даних.

Стратегії PAM для забезпечення безпеки привілейованого доступу значно розширилися, і тепер загальне визначення PAM змінилося. Зараз більшість людей розглядають PAM як управління привілейованим доступом, що охоплює ширший спектр безпеки, ніж просто керування привілейованими обліковими записами. Це означає не тільки контроль за тим, хто та які системи можуть отримати доступ до привілейованих облікових записів, але й за тим, які дії можуть виконуватись після входу в систему.

PAM містить стратегії, які дають командам безпеки можливість точніше контролювати та відстежувати дії під час привілейованих сеансів. Така стратегія включає управління паролями привілейованих облікових записів через такі методи, як керування обліковими даними, застосування принципу найменших привілеїв та

управління обліковими записами. Наприклад, процес надання доступу, двофакторна/багатофакторна автентифікація, моніторинг і запис привілейованих сеансів та запуск віддалених команд є важливими елементами цілісної програми управління привілейованим доступом.

Зазвичай організації починають свою стратегію PAM з рішень для управління привілейованими обліковими записами та сеансами (PASM), що дозволяє їм отримати видимість та контроль над своєю атакувальною поверхнею привілейованих облікових записів та зменшити їхню кількість.

Привілейовані облікові записи є шляхом до інфраструктури організації, через те, їх можна використати для доступу до серверів, бази даних, програм або робочих станцій.

Привілейовані облікові записи – це облікові записи користувачів або сервісні облікові записи, які мають підвищені дозволи, ніж у звичайних облікових записів користувачів. Ці облікові записи мають адміністративні привілеї та можуть виконувати такі важливі дії, як інсталяція програмного забезпечення, зміна параметрів системи, доступ до конфіденційних даних і керування обліковими записами користувачів.

Привілейовані облікові записи часто стають мішенню зловмисників, оскільки їх компрометація забезпечує великий контроль над системами та даними організації. Таким чином, контроль і захист привілейованих облікових записів є ключовими аспектами PAM. До привілейованих облікових записів відноситься:

Права адміністратора: користувачі з правами адміністратора мають право налаштовувати, керувати та змінювати параметри системи, встановлення програмного забезпечення та облікові записи користувачів.

Кореневий доступ: в Unix-подібних операційних системах «root» — це обліковий запис суперкористувача, який має необмежений доступ до всіх системних ресурсів і файлів.

Доступ адміністратора бази даних (DBA) : Адміністратори баз даних керують і контролюють бази даних, включаючи створення, зміну та видалення структур і даних бази даних.

Права на рівні програми: деякі програми потребують вищих прав для виконання певних завдань, наприклад доступу до конфіденційних даних або виконання операцій на системному рівні.

Права конфігурації мережі: користувачі з цими правами можуть налаштовувати параметри мережі, маршрутизатори, брандмауери та інші налаштування, пов’язані з мережею.

Керування ключами шифрування: ці користувачі можуть керувати та контролювати ключі шифрування, які захищають конфіденційні дані організації.

Контроль фізичного доступу: привілеї також можуть поширюватися на фізичний доступ, дозволяючи певним особам входити в безпечні зони (наприклад, центр обробки даних) або взаємодіяти з апаратними компонентами.

Доступ до фінансових систем: як правило, це працівники ваших фінансових і бухгалтерських відділів, ці користувачі можуть отримати доступ до вашого фінансового програмного забезпечення та систем для обробки транзакцій і виконання своїх службових функцій.

Керування хмарною інфраструктурою: адміністратори хмари мають права керувати хмарними ресурсами, віртуальними машинами, сховищем і мережевими компонентами в хмарних середовищах.

Середовища розробки та виробництва: розробники можуть мати різні рівні доступу до середовищ розробки та виробництва, що дозволяє їм створювати, тестувати та розгортати програмне забезпечення.

Рис.1.3. PAM-записи [5]

PAM є важливою практикою безпеки, яка надає організаціям значні переваги, але вона може супроводжуватися деякими з наведених нижче проблем і потенційних ризиків:

Складність: деякі рішення PAM складні в розгортанні та управлінні, що вимагає ретельного планування та інтеграції з існуючими системами. Шукаючи рішення, необхідно оцінити зручність використання продукту та легкість інтеграції, щоб переконатися, що він не буде надто обтяжувати ресурси інформаційної системи організації.

Опір користувача: користувачі з привілейованим доступом можуть протистояти реалізації рішення PAM через зміни в їхніх робочих процесах і додаткові заходи безпеки. Навчання привілейованих користувачів практики PAM покращить стан безпеки організації, допоможе їм залучитися та підтримати будь-які необхідні зміни процесу.

Неправильні конфігурації: неправильно налаштовані системи PAM можуть призвести до збоїв у критичних процесах або ненавмисного підвищення привілеїв. Неправильні конфігурації можуть виникнути через неправильне розуміння правильних налаштувань або конфліктні налаштування, тому рекомендовано обмежити кількість адміністраторів для вашого рішення PAM.

Єдина точка збою: якщо сама система PAM скомпрометована, це може призвести до серйозних наслідків, надаючи зловмисникам доступ до всіх привілейованих облікових записів. Тому вкрай важливо оцінити методи безпеки вашого постачальника PAM, щоб мінімізувати потенційні ризики та вразливі місця.

Операційні накладні витрати: PAM може додати адміністративні накладні витрати на керування та надання доступу до привілейованих облікових записів для законних користувачів.

Комплексна стратегія впровадження повністю керованої стратегії PAM (рис.1.2) складається з:

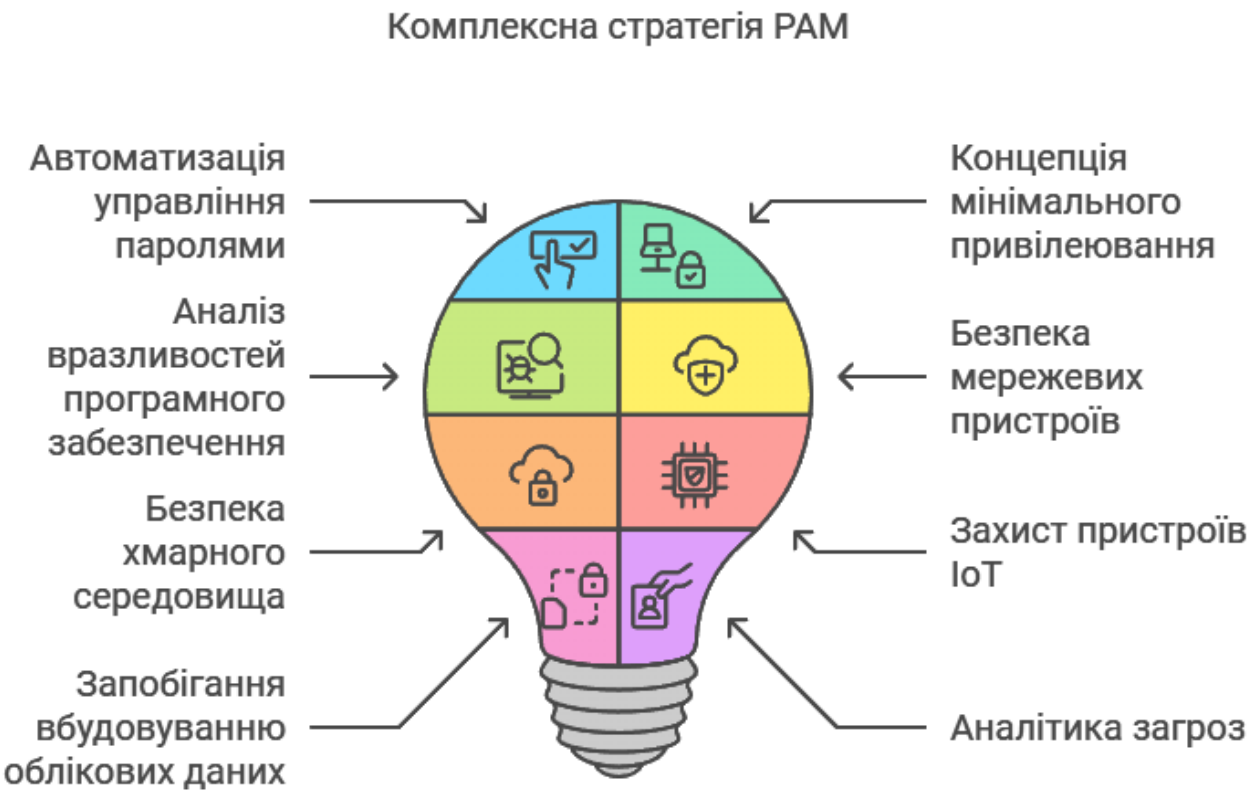

Рис.1.2. Ключові кроки до створення комплексного PAM

1. Залучення системи автоматизації до управління привілейованими паролями сприяє покращенню огляду і забезпеченню автоматичної зміни облікових записів та їх паролів. Це виключає потребу ручного втручання з боку IT-персоналу та мінімізує ймовірність помилок в адміністративних процесах. Також, завдяки коротшому життєвому циклу паролів, користувачі ніколи не отримують доступ до привілейованих паролів у будь-який момент.

2. Впровадження концепції мінімального привілеювання дозволу виконання для користувачів, призначених лише необхідні дозволи для щоденних робочих завдань. При запиті на розширення доступу, привілеї можуть надаватися тимчасово та обмежено на період виконання завдання, з подальшим відкликанням.

3. Проведення аналізу вразливостей програмного забезпечення допомагає приймати обґрунтовані рішення щодо надання привілеїв. Включення елементів

керування додатками та привілеїв у систему управління вразливістю може допомогти зменшити ризики, пов'язані з потенційними загрозами.

4. Врахування мережевих пристроїв у системі безпеки, оскільки вони також можуть стати точкою входу для зловмисників. Налаштування PAM на мережевих пристроях дозволить зменшити ризик використання стандартних облікових даних та підвищить загальний рівень безпеки.

5. Розгляд безпеки у хмарному середовищі, включаючи впровадження локальних принципів PAM у хмарну інфраструктуру, забезпечить захист конфіденційної інформації та забезпечить безпеку даних під час їх переміщення в хмару.

6. Захист пристроїв Інтернету речей (IoT) шляхом впровадження автоматизованих рішень PAM допоможе знизити ризик кібератак і зберегти конфіденційні дані.

7. Запобігання вбудовуванню облікових даних у програми і веб-сайти може бути досягнуто за допомогою належної політики PAM, що дозволяє керувати доступом до облікових даних з точністю і безпекою.

8. Використання привілейованої аналітики загроз (PTA) для моніторингу та оцінки ризиків поведінки користувачів, а також надання сповіщень у разі виявлення підозрілої або ризикованої діяльності.

9. Інтеграція привілейованих облікових записів для спільного керування користувачами між системами на базі Unix і Windows.

10. Інтеграція стеку ідентифікаційних даних для спільної роботи інструментів керування ідентифікацією та доступом, з метою посилення контролю доступу та зменшення ризику атак.

Як було сказано, організаціям необхідно застосувати проактивний, цілісний підхід до управління привілейованим доступом, щоб досягти успіху у впровадженні PAM.

Реалізація вищезазначених кроків може допомогти мінімізувати зловживання привілеями, але це не буде остаточним рішенням безпеки. Оскільки використання привілейованих облікових записів зростає, організаціям вкрай

необхідно співпрацювати з постачальниками рішень для кібербезпеки, які розглянемо в наступному підрозділі, щоб розробити ще більш досконалу стратегію PAM, яка встановлює ширші межі та створює відповідний кіберзахист.

1.2. Аналіз проблеми використання привілейованого доступу

Прийнятих на даний момент методів безпеки та рішень загалом недостатньо для повної безпеки використання привілейованого доступу. Згідно з результатами опитування, 80% організацій стикалися з порушенням політики привілейованого доступу протягом попереднього року (рис. 1.3.), і ці цифри відображають лише відомі порушення політики. Справжні результати, ймовірно, дещо вищі, оскільки багатьом організаціям бракує інструментів моніторингу, необхідних для виявлення всіх порушень.

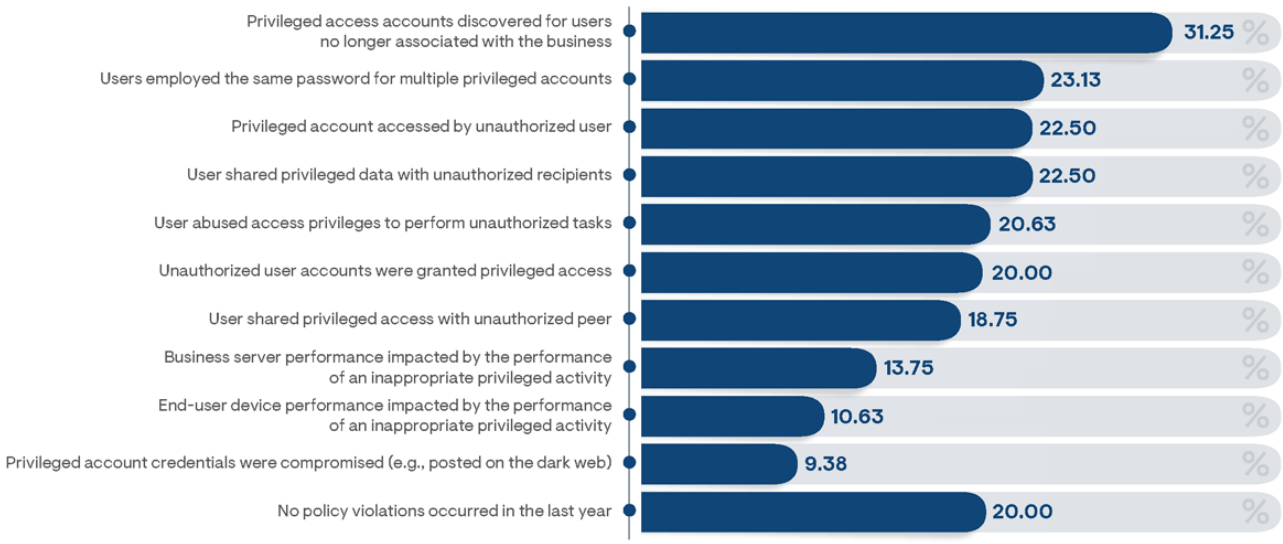

Рис. 1.3. Статистика порушень PAM

Серед респондентів, яким вдалося виявити випадки порушення, найчастіше відзначалося виявлення активних привілейованих облікових записів колишніх співробітників або підрядників. Часто буває так, що IT-адміністратори не знають

про всі привілейовані облікові записи, які були надані користувачам під час їх припинення. Ці нерозпізнані облікові записи можуть залишатися доступними та активними необмежений час, що робить їх основними цілями для зловмисників, які шукають таємні методи отримання привілейованих облікових даних.

Респонденти з великого бізнесу (37%) частіше відзначали такі види порушень, ніж респонденти з малого бізнесу (25%), ймовірно, через більшу щільність плинності працівників, яка спостерігається у великих організаціях. Більше половини (55%) усіх респондентів з організацій, які використовують безкоштовне або недороге сховище паролів як основний метод контролю привілейованого доступу, повідомили про випадки виявлення привілейованих облікових записів для колишніх користувачів за останній рік, що вказує на те, що він був найменш ефективним метод увімкнення видимості привілейованого облікового запису.

Серед 23% респондентів минулого року також були виявлені випадки використання користувачами одного пароля для кількох привілейованих облікових записів. У цих випадках зловмисник, якому вдалося отримати пароль (наприклад, за допомогою грубої сили, фішингу або атак інструментів злому) на одну бізнес-систему, зможе використати його для отримання доступу до додаткових бізнес-систем. Пов’язані інциденти найчастіше відзначалися серед респондентів фінансових установ (36%). Також про них найбільше повідомили організації, які покладаються на власні інструменти операційної системи кінцевих точок для захисту привілейованих облікових записів, очевидно тому, що вони пропонують найменш ефективний контроль пароля.

Найбільш явне порушення політики привілейованого доступу — привілейований обліковий запис, доступ до якого має авторизований користувач — було виявлено більш ніж 22% респондентів. Відповідні інциденти вдвічі частіше траплялися у великих підприємствах, ніж у малих (від 31% до 14% респондентів відповідно). Високий рівень інцидентів для цього порушення особливо відзначили респонденти з фінансової (44%) та охорони здоров’я (38%) галузей. Організації, які використовують безкоштовні або недорогі рішення для зберігання паролів, а також

організації, які покладаються на прості спільні електронні таблиці для керування привілейованим доступом, найімовірніше стикалися з несанкціонованим використанням привілейованого облікового запису, як повідомили приблизно 30% респондентів з кожної демографічної групи. Цікаво, що більше половини організацій, які надають привілейований доступ особам, які не є адміністраторами, повідомили про несанкціоноване використання привілейованих облікових записів, що вказує на те, що кінцеві користувачі частіше використовують погані методи безпеки та недостатньо керовані у більшості компаній.

Високий рівень випадків порушень не залишився непоміченим менеджерами з IT та безпеки, оскільки 93% респондентів зазначили, що вони не впевнені, що прийняте ними рішення запобіжить усім порушенням безпеки привілейованого доступу. Було зазначено, що вищий рівень впевненості досягається завдяки використанню рішень, які активно відстежують і керують засобами контролю доступу, включаючи IAM, мережеве керування та платформи, призначені для PAM (рис. 1.4). Навпаки, організації, які використовують базові інструменти, включаючи спільні електронні таблиці, платформи керування кінцевими точками та власно створені сценарії, досягли значно нижчого рівня впевненості в безпеці своїх рішень із привілейованим доступом.

Організації, які зазнали порушень політики привілейованого доступу, переважно вказали, що зазнали прямих бізнес-наслідків, пов’язаних із порушенням. Загалом близько 87% респондентів опитування з організацій, які порушили правила, повідомили про конкретний вплив на бізнес-операції (Рисунок 12). Найчастішими (і найменш вражаючими) були випадки доган співробітників. Проте кожен п’ятий респондент повідомив, що працівника було звільнено внаслідок порушення привілейованого доступу. Очевидно, що користувачі поділяють відповідальність за забезпечення доступу до свого авторизованого привілейованого доступу разом із своїм бізнесом і несуть однакову відповідальність за будь-які наслідки, спричинені зловживанням їхнім підвищеним доступом.

Серед наслідків для бізнес-операцій учасники опитування найчастіше відзначали недотримання нормативних вимог і розкриття конфіденційної бізнес-IT-інформації. Ці два виклики нерозривно пов'язані, тому що останній, безсумнівно, призведе до першого. Приблизно кожна п'ята компанія, яка зазнала порушення політики, зазнала серйозного впливу на загальну ефективність бізнесу, включаючи пряму втрату доходу, втрату клієнтів та/або шкоду репутації компанії. Хоча це відзначили лише 14% респондентів опитування, раптова неможливість отримати страхування кібербезпеки через випадок порушення є відносно новим наслідком, який починає набувати все більшого значення.

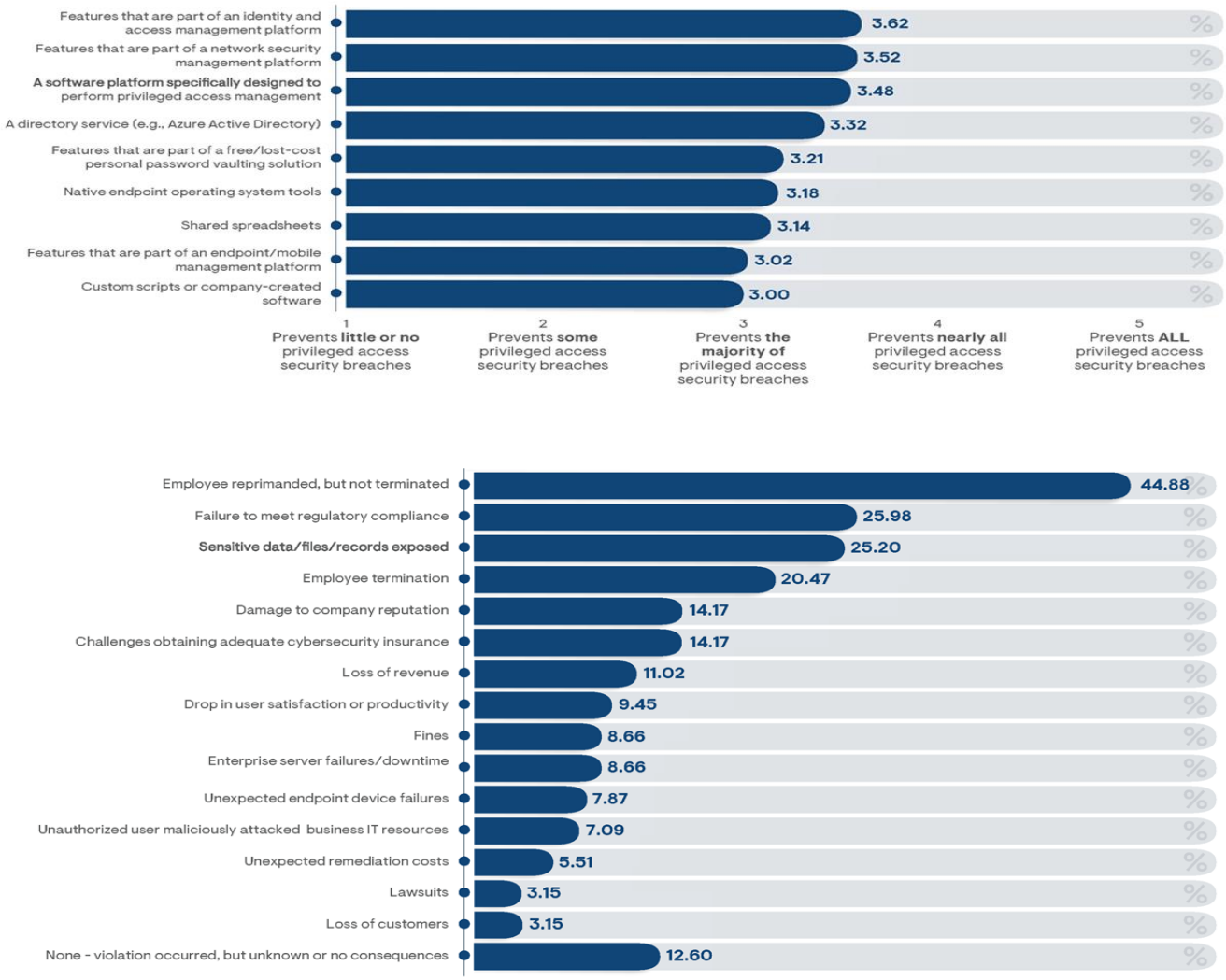

Рис.1.4. Середній рівень впевненості респондентів щодо спроможності їх інструментів запобігати порушенням безпеки привілейованого доступу, вказаний респондентами.

Високу частоту порушень політики привілейованого доступу та їх наслідки можна загалом пояснити неефективними або погано розгорнутими рішеннями PAM. Перешкоди для впровадження більш ефективних методів керування привілейованим доступом пов'язані, головним чином, із зростанням складності управління IT. Зокрема, 57% респондентів опитування вказали, що забезпечити інтеграцію прийнятого ними PAM-рішення зі сторонніми платформами помірно або дуже важко (рис. 1.5). Багато комерційно доступних хмарних і корпоративних програмних продуктів містять власні процеси доступу, розроблені для незалежної роботи. Для безперебійної роботи з централізованим рішенням PAM часто потрібна розробка точок інтеграції з використанням доступних API або SDK, які потрібно підтримувати та зазвичай не повністю підтримуються жодним із постачальників рішень. Було визначено, що інтеграція є найскладнішою для організацій, які використовують користувацькі сценарії або спільні електронні таблиці для керування привілейованим доступом, і її найпростіше ввімкнути компаніям, які прийняли спеціальну платформу PAM.

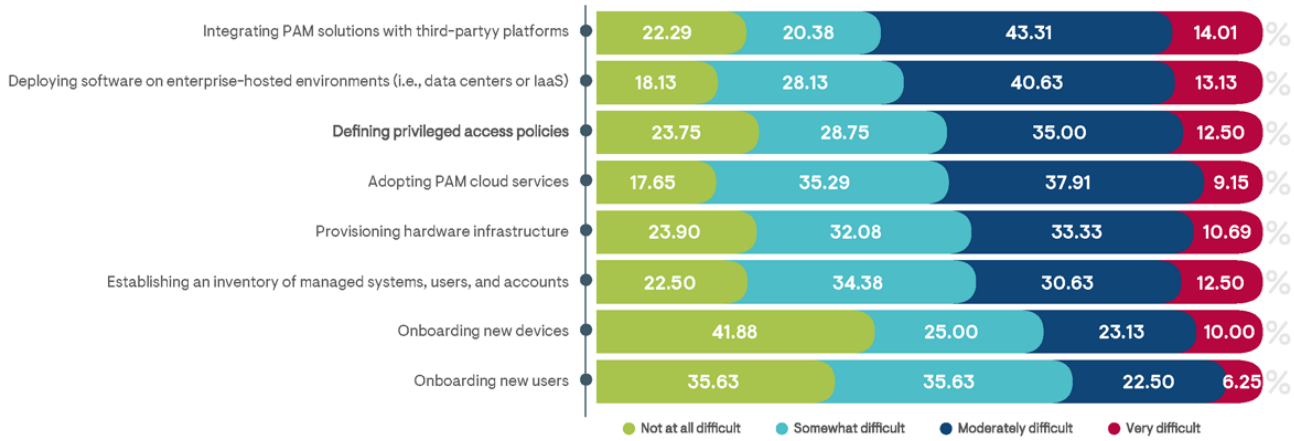

Рис. 1.5. Відсоток респондентів опитування, які вказали на рівень труднощів із процесами розгортання для поточного рішення PAM їхньої організації

Більше половини респондентів опитування також відзначили, що процеси розгортання корпоративного програмного забезпечення PAM є помірними або дуже складними. Це включає придбання та інсталяцію компонентів складної

інфраструктури, таких як сервери, мережі, бази даних і засоби контролю безпеки. Не дивно, що малому бізнесу було особливо складно розгортати локальні рішення PAM: 86% респондентів вказали, що це помірно або дуже складно. Розміщені в хмарі PAM-рішення, які включають ресурси, попередньо зібрані разом із службою, були значно легшими для розгортання, ніж корпоративні рішення.

Більшість респондентів відзначили, що процеси адаптації нових користувачів і пристроїв відносно прості. Однак єдиним винятком із цього є організації, які використовують спільні електронні таблиці для керування привілейованим доступом, оскільки було зазначено, що вони мають значні проблеми з підключенням нових пристроїв, причому 57% вказали, що це помірно або дуже важко. Відстеження привілейованого доступу за допомогою електронної таблиці вимагає постійних оновлень вручну, що може бути важким для адміністраторів, яким потрібно виконувати інші критичні завдання з управління IT.

Загалом повсякденна діяльність з керування PAM виявилася менш ефективною, ніж завдання початкового розгортання. За словами респондентів, найскладніші завдання адміністрування включають забезпечення того, щоб користувачі постійно використовували надійні та безкомпромісні паролі (Рис. 1.6).

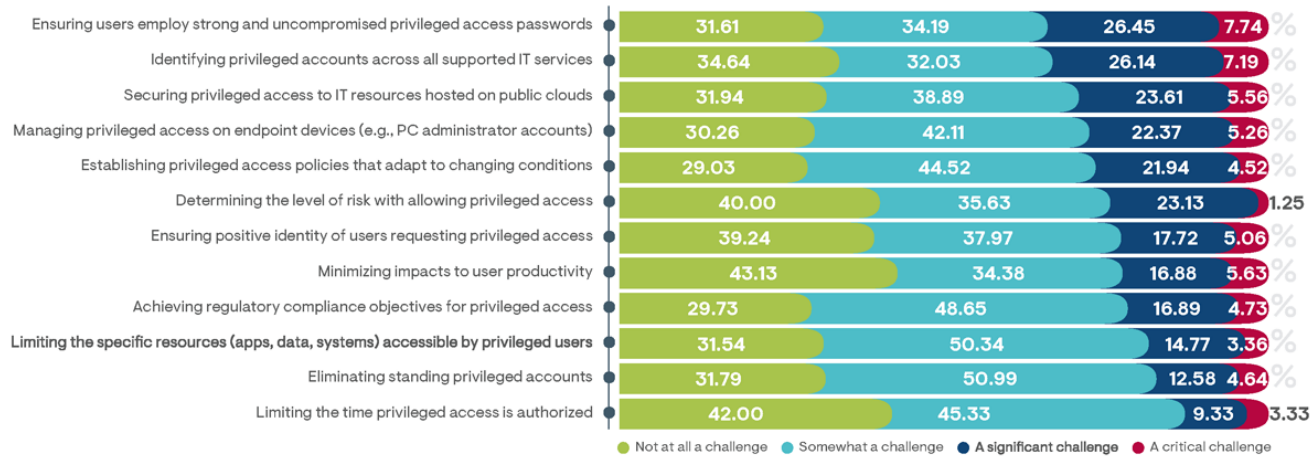

Рис.1.6. Відсоток респондентів опитування, які вказали на рівень труднощів із процесами розгортання для поточного рішення PAM їхньої організації

Це включає перевірки для виявлення слабких паролів (наприклад, шляхом тестування таблиць паролів за допомогою програмного забезпечення для злому) і виявлення зламаних паролів, опублікованих у темній мережі. Труднощі із забезпеченням безпеки паролів особливо відзначили організації, які підтримують PAM за допомогою недорогого рішення для зберігання паролів або спільних електронних таблиць.

Були також вказані еквівалентні проблеми зі спробами ідентифікувати привілейовані облікові записи в усіх підтримуваних IT-службах. Більшість сучасних складних IT-середовищ розміщують IT-сервіси на різноманітних корпоративних серверах, хмарних ресурсах і ресурсах кінцевих точок, і кожен може мати власні унікальні облікові записи привілейованого доступу та процеси адміністрування. Централізоване визначення користувачів, до яких ресурсів мають привілейований доступ, може зайняти надзвичайно багато часу без централізованої платформи автоматичного та постійного моніторингу привілейованих облікових записів і авторизацій. Дійсно, 46% організацій, які прийняли спеціальну платформу PAM, повідомили, що вони взагалі не вважають це проблемою, що вказує на те, що цей підхід є найефективнішим для забезпечення видимості привілейованого облікового запису.

Враховуючи широкі та зростаючі вимоги до контролю привілейованого доступу, не дивно, що більшість організацій розробили довгострокові цілі щодо включення PAM. У середньому респонденти опитування повідомили, що вони пройшли половину запланованого розгортання можливостей PAM, причому великі компанії вказали, що вони просуваються у своїх планах дещо далі, ніж менші підприємства (рис. 1.7.). Було відзначено, що фінансові установи найдальше просунулися у своєму шляху PAM (у середньому 59% шляху), а професійні послуги – як найбільше відстаючих (в середньому 38% шляху). Лише близько 5% від загальної кількості респондентів вказали, що вони досягли своїх цілей PAM, і лише 2% повідомили, що вони ще не почали виконувати свої плани впровадження PAM.

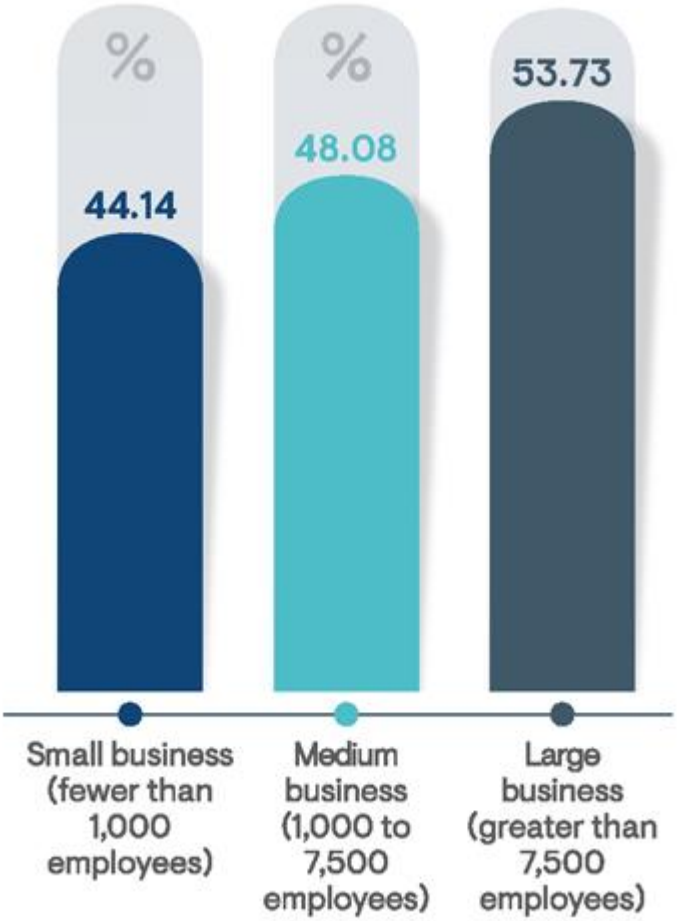

Рис. 1.7. Середній відсоток запланованих організацій, які респонденти вже розгорнули опитування можливостей PAM, у своїй організації, сегментований за розміром бізнесу

1.3. Аналіз рішень управління привілейованим доступом до інформаційної системи організації

Більшість організацій структурують свої системи за рівнями відповідно до серйозності можливих наслідків в разі порушення або неправильного використання. Чим вищий рівень, тим більші наслідки може мати подібне порушення.

Рішення PAM допомагають IT-адміністраторам і адміністраторам безпеки контролювати та захищати привілейований доступ, дозволяючи їм надавати «точно вчасно» доступ до систем високого рівня. Це означає, що користувачам надаються

підвищені дозволи лише до тих пір, поки вони потрібні для виконання їхньої роботи. Після виходу з системи високого рівня дозволи скасовуються. Ці дозволи також можуть бути обмежені за часом; користувач матиме доступ протягом певного періоду часу, перш ніж йому доведеться шукати оновлений дозвіл. Це захищає критично важливі бізнес-системи від несанкціонованого доступу та сприяє кращому управлінню відповідно до норм захисту даних.

Розглянемо найбільш відомі рішення привілейованого доступу.

ARCON PAM пропонує низку основних функцій і функцій, необхідних для досягнення моделі зрілості PAM. Повноцінне рішення з масштабованою архітектурою забезпечує неприступну безпеку привілейованої ідентифікації. Банківські організації, державні установи, мережі охорони здоров'я серед багатьох вертикальних ринків довіряють ARCON PAM для створення надійної системи IAM і відповідності.

Рішення ARCON для управління ризиками розроблені для захисту даних і конфіденційності шляхом прогнозування ситуацій ризику, захисту організацій від цих ризиків і запобігання їх прогресуванню в інциденти. Управління привілейованим доступом (PAM) ARCON дозволяє групам безпеки підприємства захищати та керувати всім життєвим циклом своїх привілейованих облікових записів. Він захищає привілейовані облікові дані від атак скомпрометованих інсайдерів і сторонніх кіберзлочинів. [3, 7, 8]

ARCON PAM має безпечне сховище паролів, яке автоматизує часті зміни паролів. Сховище генерує та зберігає надійні динамічні паролі, доступ до яких мають лише авторизовані користувачі. Користувачі повинні пройти багатофакторну автентифікацію (MFA), щоб отримати доступ до сховища. ARCON пропонує власну програмну перевірку одноразового пароля (OTP) для перевірки особи користувачів, і цей інструмент інтегрується зі сторонніми рішеннями автентифікації, якщо організація хоче створити рівні автентифікації навколо сховища. Безпека MFA дозволяє ARCON PAM запуск єдиного входу (SSO) для доступу до всіх критично важливих систем без користувачів, які повинні ділитися своїми обліковими даними. Це робить процес входу більш ефективним, водночас

захищаючи важливі дані від загрози злому пароля. Нарешті, увесь привілейований доступ здійснюється точно вчасно, що зменшує поверхню загрози, віддаючи перевагу доступу за потреби над постійними привілеями.[3]

Розширений моніторинг сеансів дає адміністраторам повне уявлення про те, хто використовує середовище привілейованого доступу та чому, що дозволяє швидше зменшувати ризики. ARCON PAM також забезпечує повний контрольний журнал привілейованих дій, а також звіти та аналітику результатів за допомогою механізму звітності рішення. Це дозволяє керівникам і аудиторам за потреби оцінювати статус відповідності організації.

BeyondTrust — це комплексне рішення для керування привілейованим доступом, яке пропонує привілейоване керування паролями та сеансами, безпечний віддалений доступ і керування вразливими місцями. Його перевага полягає в наданні обширної аналітики загроз, що значно покращує його здатність пом’якшувати потенційні ризики безпеці.

BeyondTrust має майстерність у сфері аналізу загроз. Його здатність надавати детальну інформацію відрізняє його від інших рішень. Виходячи з цього BeyondTrust кваліфікується як «найкраще рішення для розгорнутої аналітики загроз», оскільки пропонує винятковий рівень деталізації виявлення та моніторингу загроз, що є критично важливим у сучасному ландшафті кібербезпеки.

Такі функції BeyondTrust, як розширені звіти, можливості інформаційної панелі та аналітика в реальному часі, справді варті уваги. Це сприяє поглибленому аналізу потенційних загроз. BeyondTrust також пропонує інтеграцію з широким спектром систем і програм, починаючи від інструментів ITSM, таких як ServiceNow, і закінчуючи рішеннями SIEM, такими як Splunk, що ще більше підвищує його корисність. [3]

Symantec є провідним виробником рішень для запобігання втраті корпоративних даних (DLP), захисту кінцевих точок і веб-безпеки. Symantec Privileged Account Management (PAM) — це рішення PAM, створене для того, щоб допомогти організаціям легше відстежувати та керувати доступом до корпоративних облікових записів високого рівня, щоб зменшити ризик порушення

облікових даних і забезпечити відповідність галузевим стандартам, таким як PCI-DSS. [3]

Broadcom (Symantec)

Broadcom (Symantec) є нішевим гравцем у цьому магічному квадранті. Його PAM-продуктом є Symantec Privileged Access Management, який доступний як віртуальний або апаратний пристрій і включає в себе PASM, PEDM, AAPM і управління секретами в комплексі. Broadcom не пропонує CIEM. Broadcom має значну кількість клієнтів у Північній Америці, EMEA та APAC. Пункти дорожньої карти з моменту останнього Magic Quadrant включають незначні вдосконалення існуючих функцій, як-от відкриття та керування секретами, а також впровадження нового шлюзу PAM на основі браузера. Broadcom не відповів на запити щодо додаткової інформації. Тому аналіз Gartner базується на інших надійних джерелах.

Сильні сторони

Продукт : Broadcom пропонує дуже конкурентоспроможний продукт PEDM для Windows і UNIX/Linux. Продуктивність і масштабованість , доступність і можливості відновлення є сильними для PASM, включаючи відмінні функції кластеризації та високої доступності , які підтримують додавання вузлів без необхідності відключати кластер.

Ціноутворення : ціни на Symantec PAM є конкурентоспроможними, причому ціни майже в усіх сценаріях нижчі , а іноді й значно нижчі за середні для ринку в цілому. Крім того, Broadcom пропонує своїм провідним клієнтам портфоліо ліцензійних угод, які можуть запропонувати додаткову економію.

Географічна стратегія: Broadcom підтримує сильну глобальну присутність і продовжує пропонувати цілеспрямовану підтримку своїм клієнтам PAM у різних регіонах .

Продукт: Broadcom має вище середнього рівня продуктивності та доступності. Він пропонує надійну підтримку для дуже великих реалізацій PAM із спрощеним підходом до масштабування проксі-серверів, переходів або бастіонних серверів , а також може підтримувати велику кількість одночасних сеансів для масштабування підприємства.Symantec PAM зберігає всі привілейовані облікові

дані, включаючи паролі адміністратора та адміністратора, а також ключі SSH, у безпечному сховищі. Користувачі повинні підтвердити свою особу за допомогою двофакторної автентифікації, перш ніж їм буде надано доступ до сховища, а облікові дані автоматично змінюються відповідно до налаштованих адміністратором політик, щоб забезпечити дотримання стандартів захисту даних і допомогти запобігти порушенням у результаті використання постійних облікових даних.

Symantec PAM постійно стежить за діяльністю привілейованих користувачів, застосовуючи методи машинного навчання для порівняння поточних дій з минулими діями, щоб виявити підозрілу або аномальну поведінку.

Symantec Privileged Access Management для середніх і великих організацій, які бажають запровадити рішення PAM, щоб запобігти витоку облікових даних і боковим атакам компрометації облікових записів.

CyberArk — це визнане ім’я в галузі управління привілейованим доступом, що пропонує широкий набір рішень, спрямованих на захист бізнесу на різних платформах і середовищах. Його всеосяжний характер гарантує, що організації можуть керувати, контролювати та відстежувати привілейовані облікові записи, таким чином мінімізуючи потенційні вразливості безпеки.

CyberArk має широкий спектр пропозицій, які разом складають комплексний пакет рішень. Цей цілісний підхід вирізняє CyberArk, тому він добре підходить для компаній, які шукають комплексну платформу, а не часткові рішення.

Ця широта функцій і послуг є причиною того, чому я вважаю, що CyberArk є «найкращим із комплексним набором рішень».

Функції CyberArk поширюються від виявлення привілейованого облікового запису, надання та деініціалізації до ізоляції сеансу, моніторингу та аналізу загроз. Його хмара привілеїв виділяється як важлива пропозиція, забезпечуючи безпеку привілейованого доступу як послугу. CyberAr*k* інтегрується з безліччю програм і платформ, включаючи Windows, Unix/Linux, бази даних, віртуальні середовища та мережеві пристрої.

CyberArk також пропонує розширену версію своєї Core Privileged Access Security, яка включає централізовано керовані детальні засоби контролю доступу для захисту серверів із найменшими привілеями та моніторингу мережі на наявність загроз для контролерів домену. Обидва ці модулі повністю інтегруються зі стандартним рішенням. Рішення CyberArk пропонує варіанти локального, хмарного та SaaS розгортання, що робить його придатним для всіх організацій, незалежно від стану переходу на хмару.

Delinea, провайдер кібербезпеки, що народився в результаті злиття Thycotic і Centrify у 2020 році, є фахівцем з надання рішень для управління доступом на рівні підприємства.

Delinea — це програмна платформа безпеки, розроблена, щоб допомогти організаціям керувати привілейованим доступом. Ця платформа спрощує керування привілеями в IT-середовищі організації, що робить її найкращим вибором для компаній, які прагнуть ефективного керування привілеями.

Делінея є лідером у цьому магічному квадранті. Його пропозиція PAM складається з продукту Delinea Platform , доступного як SaaS, який включає разом функціональні можливості PASM, PEDM, RPAM і CIEM. Окремі варіанти включають Secret Server для PASM (SaaS або програмне забезпечення), PEDM з Privilege Manager (SaaS або програмне забезпечення, кінцеві точки Windows і macOS) і Server Suite (кінцеві точки UNIX/Linux).

DevOps Secrets Vault — це продукт для керування секретами. Раніше в 2024 році Delinea придбала Authomize, що покращує існуючі можливості CIEM, і FastPath (також на початку 2024 року), який, за словами Delinea, покращить JIT і функції керування життєвим циклом. Діяльність Delinea є географічно диверсифікованою, хоча більшість її клієнтів знаходяться в Північній Америці, потім у Європі. Пункти дорожньої карти, починаючи з останнього магічного квадранта, включають розширення функцій CIEM для програм CSP і SaaS, а також можливість керувати іншими сховищами CSP і сторонніх виробників для вдосконалення управління секретами.

Delinea має дуже компетентну пропозицію PEDM для UNIX/Linux, яка ввійшла до числа найкращих постачальників серед оцінюваних.

Загальна життєздатність: Дохід і зростання кількості клієнтів Delinea були одними з найвищих серед усіх постачальників, які брали участь у цьому дослідженні.

Клієнтський досвід: клієнти Delinea постійно відзначають зручність продукції компанії. Він пропонує уніфіковані механізми та з'єднувачі для єдиної площини керування та повне охоплення звітів про стан здоров'я.

Географічна стратегія: Delinea створила потужну географічну присутність і має намір розширити охоплення глобальних клієнтів шляхом посилення локальної операційної підтримки в Азіатсько-Тихоокеанському регіоні, Японії та Латинської Америки.

Gartner визначає керування привілейованим доступом (PAM) як інструменти, які забезпечують підвищений рівень технічного доступу через керування та захист облікових записів, облікових даних і команд, які використовуються для адміністрування або налаштування систем і програм. Інструменти PAM — доступні як програмне забезпечення, SaaS або апаратне забезпечення — керують привілейованим доступом як для людей (системних адміністраторів та інших), так і для машин (систем або програм). Gartner визначає чотири різні категорії інструментів для інструментів PAM: керування привілейованими обліковими записами та сеансами (PASM), керування підвищенням прав і делегуванням (PEDM), керування секретами та керування правами доступу до хмарної інфраструктури (CIEM) (рис.1.8).

Привілейований доступ — це доступ, що перевищує звичайний рівень, наданий бізнес- користувачам . Це дозволяє користувачам скасовувати існуючі засоби контролю доступу, змінювати конфігурації безпеки або вносити зміни, що стосуються кількох користувачів або систем. Оскільки привілейований доступ може створювати, змінювати та видаляти IT-інфраструктуру разом із даними компанії, що містяться в цій інфраструктурі, це становить катастрофічний ризик. Таким чином, керування привілейованим доступом є критично важливою

функцією безпеки для кожної організації. Користувачі з нормальним рівнем контролю доступу не можуть ефективно керувати привілейованим доступом, тому потрібен певний набір процедур та інструментів. Інструменти PAM зосереджуються або на привілейованих облікових записах, або на привілейованих командах .

Інструменти PAM допомагають організаціям виявляти привілейовані облікові записи, якими користуються люди та машини. Інструменти PAM захищають ці облікові записи, змінюючи та зберігаючи їхні облікові дані (наприклад, паролі, ключі), а також надаючи делегований доступ до них у контрольований спосіб . Для інтерактивних облікових записів, якими користуються люди, інструменти PAM допомагають забезпечити багатофакторну автентифікацію та явний довірчий віддалений доступ через механізми керування сеансом, щоб увімкнути привілейоване використання облікового запису без розкриття облікових даних. Для неінтерактивних облікових записів, які використовуються машинами, інструменти PAM захищають обробку привілейованих облікових даних, щоб вони не були відкритими в стані спокою.

Інструменти PAM також забезпечують керування командами, дозволяючи виконувати лише певні дії, і за бажанням можуть тимчасово підвищувати привілеї користувача, щоб дозволити виконання команд у привілейованому контексті.

Інструменти PAM забезпечують видимість і контроль використання привілейованого облікового запису та команд шляхом відстеження та запису привілейованого доступу для аудиту. Це включає детальний запис сеансу, щоб допомогти зрозуміти не тільки хто використовував який привілейований обліковий запис і коли, але й що вони робили.

Елементи керування, надані інструментами PAM, можуть реалізовувати своєчасне керування привілеями для забезпечення дотримання принципу найменших привілеїв: користувачі повинні мати правильний рівень доступу до потрібного ресурсу з правильної причини та в правильний час.

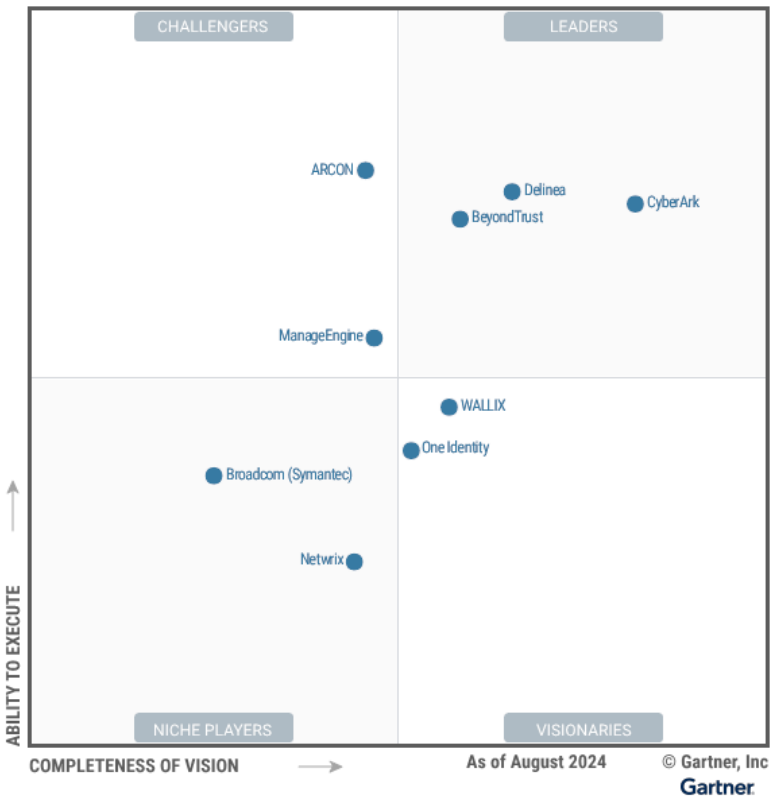

Рис.1.8. Лідери PAM

https://www.gartner.com/doc/reprints?id=1-2IRCE33T&ct=240909&st=sb

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

Висновки до розділу 1

1. Проведено аналіз проблеми управління привілейованим доступом, яке призначене для організації контролю, щодо захисту привілейований доступ, дозволяючи надавати «точно вчасно» доступ до систем високого рівня.

3. Обґрунтувано вибір рішення привілейованого доступу на основі рішень, які є лідерами ринку кібербезпеки, Обране рішення дозволить організаціям управляти привілейованими записами відповідно до їхніх потреб. Для подальшого дослідження було обрано рішення Delinea PAM.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ РІШЕННЯ DELINEA

2.1. Етапи планування привілейованого доступу рішення Delinea

Правильне налаштування управління привілейованим доступом вимагає початкового плану і постійної програми. Першим кроком є визначення того, які привілейовані облікові записи мають бути пріоритетними організації, і переконайтися, що люди, відповідальні за керування привілейованими обліковими записами, чітко розуміють їх прийнятне використання та обов'язки.

Керування привілейованим доступом (PAM) є головним пріоритетом для багатьох організацій у всьому світі, оскільки кіберзлочинці продовжують націлюватися на привілейовані облікові записи, щоб отримати доступ, пересуватися по мережі та здійснювати зловмисну діяльність.

У зв'язку з критичним впливом привілейованих облікових записів організації повинні впроваджувати найкращі практики PAM для захисту та зменшення ризиків привілейованих облікових записів у традиційних середовищах і хмарній інфраструктурі.

Організації з найпривілейованішими обліковими записами повинні захистити:

Адміністраторів домену

Місцевіх адміністратори

Кореневі облікові записи

Сервісні облікові записи

Мережеві облікові записи, такі як CISCO Enable

Облікові записи програми

Облікові записи автоматизації для виконання робочих навантажень.

Перед тим як впровадити рішення керування привілейованим доступом, необхідно провести планування основних кроків [1].

1. Визначити, які важливі функції залежать від даних, систем і доступу.

2. Визначити кому потрібен доступ до ваших привілейованих облікових записів.

3. Визначити сторонніх підрядників, яким потрібен доступ.

4. Встановити часові вікна для використання привілейованого облікового запису.

5. Розуміти шляхи вирішення, якщо станеться злам системи привілейованого доступу.

Багато організацій є не готовими до зламу облікового запиу, і зазвичай за умовчанням просто змінюють паролі привілейованого облікового запису або вимикають привілейований обліковий запис. Цього недостатньо безпеки. Комплексний набір інструментів реагування на інциденти допоможе запобігти перетворенню кібератаки в кіберкатастрофу, забезпечуючи врахування ключових питань, таких як:

– кроки, які необхідно вжити до того, як станеться інцидент, щоб переконатися, що люди готові діяти;

– індикатори компрометації, які допомагають виявити привілейовану атаку;

– дії, які необхідно вжити під час кожної фази інциденту, щоб стримати збиток;

– стратегії, які допоможуть вам продовжувати нормальний бізнес навіть під час нападу.

6. Визначити ризик того, що привілейовані облікові записи будуть викриті або зловживаються інсайдером.

7. Знати політику IT-безпеки, яка чітко охоплює керування привілейованим доступом.

8. Розуміти як дотримуватися державних чи галузевих норм.

2.2. Життєвий цикл управління привілейованим доступом

Диспетчер життєвого циклу облікових записів (ALM) контролює створення, керування та виведення з експлуатації облікових записів служби Active Directory, які працюють у мережі вашої організації. ALM зменшує розповсюдження облікових записів служби та підвищує безпеку, посилюючи керування та створюючи підзвітність за допомогою дозволів на основі ролей. Залежно від ролі користувача, він може запитувати, затверджувати, надавати, керувати обліковими записами служб і видаляти їх[4].

ALM керує обліковими записами служби, призначаючи кожен обліковий запис користувачеві у вашій організації. ALM використовує чотири ролі для визначення дозволів користувача та визначення підзвітності. Роль користувача визначає, як він взаємодіє з ALM і обліковими записами служби.

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

2. Системний адміністратор – системний адміністратор має повний доступ до конфігурації та керування ALM. Вони можуть створювати користувачів, ролі, групи та робочі процеси та керувати ними.

3. Запитувач – Запитувачі можуть подати запит на створення нових облікових записів служби.

4. Схвалювач – схвалювачі переглядають запити на нові сервісні облікові записи та схвалюють або відхиляють їх надання.

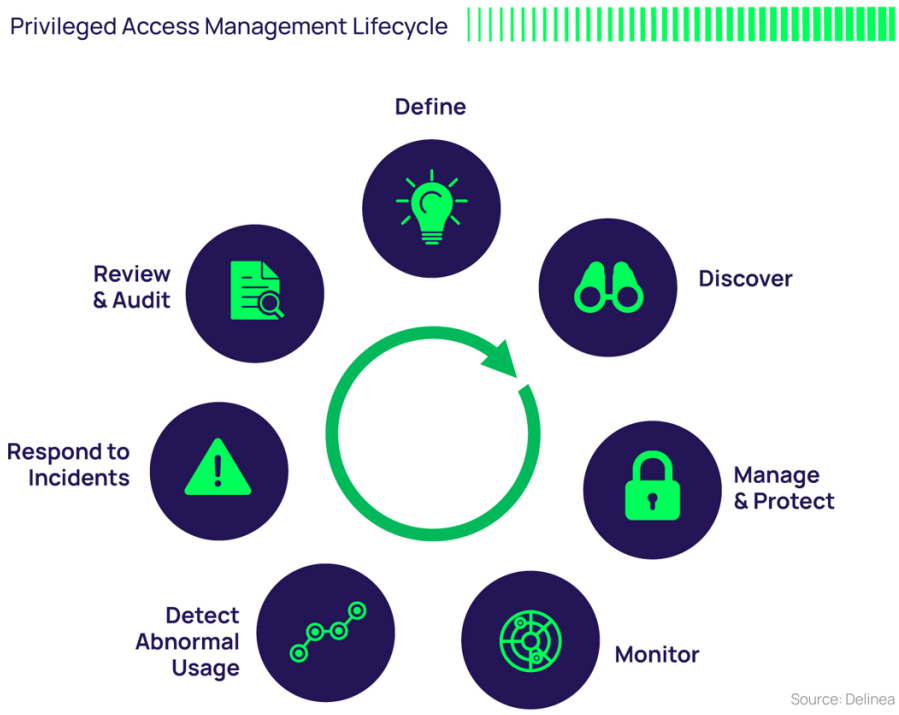

Рис.2.1. Життєвий цикл управління привілейованим доступом Delinea [4]

Ось етапи життєвого циклу PAM:

1. Визначати

Визначити та класифікувати привілейовані облікові записи. Всі бізнес-функції організації залежать від інформації, систем і наданого доступу, і залежать від цих об’єктів.

Відповідно від розробленої політики безпеки організації, яка включає привілейовані облікові записи. Необхідно мати робоче розуміння того, хто має привілейований доступ і як він використовується. Тому необхідно розглядати привілейовані облікові записи окремо, чітко визначаючи привілейований обліковий запис і викладаючи правила прийнятного використання.

2. Виявляти

Виявляйте для себе свої привілейовані облікові записи. Автоматизоване програмне забезпечення управління привілейованим доступом дозволяє ідентифікувати всі привілейовані облікові записи, здійснювати їх безперервне виявлення.

3. Управляти і захищати

Управляти, відстежувати та контролювати доступ до привілейованого облікового запису можна за допомогою паролем. Рішення для управління паролями повинно автоматично виявляти та зберігати привілейовані облікові записи.

Необхідно обмежити доступ IT-адміністраторів до інформаційної системи. Розробити політику найменших привілеїв, щоб забезпечити найменші привілеї на кінцевих точках, не порушуючи бізнес-операції.

4. Моніторинг

Необхідно відстежувати та записувати сеанси активності привілейованого облікового запису. Це допоможе забезпечувати відповіднк поведінку та уникати помилки користувачів, тому що вони будуть знати що їх діяльність контролюється. У разі виникнення інциденту, моніторинг використання привілейованого облікового запису допоможе аналітикам з кібербезпеки виявити причину.

5. Виявлення ненормального використання

Відстеження доступу та активність привілейованих облікових записів у режимі реального часу допоможе виявити ймовірну компрометацію облікового запису та потенційне зловживання користувачами.

6. Реагувати на інциденти

Необхідно підготувати план реагування на інцидент, на випадок, якщо привілейований обліковий запис буде зламано. Такі дії, як зміна паролів привілейованого облікового запису або вимкнення привілейованого облікового запису буде недостатня, якщо привілейований обліковий запис було зламано.

7. Аналіз та аудит

Постійний моніторинг привілейованого облікового запису за допомогою перевірок і звітів дозволить виявляти незвичайну поведінку. Це може свідчити про порушення або неправильне використання привілейованого запису. Такі автоматизовані звіти допоможуть відстежити причини виникнення інцидентів безпеки, а також продемонструють відповідність політикам безпеки і відповідності нормам. Зокрема, привілейований аудит облікового запису надає відповідні

показники безпеки та необхідну інформацію організації, яка необхідна керівникам для прийняття важливих бізнес-рішень.

2.3. Архітектура та компоненти платформи Delinea PAM

Архітектура платформи Delinea PAM – це хмарна архітектура, яка може підвищити стійкість організацій до кібернетичного середовища за умови дотримання певних умов. Хмарні обчислення пропонують високомасштабовану та гнучку інфраструктуру для IT та безпеки. Власні хмарні архітектури мають потенціал для покращення аварійного відновлення та безперервності бізнесу, забезпечуючи безперервне резервне копіювання, відновлення після відмови та відновлення даних.

Платформа Delinea надає безліч переваг, зокрема:

Зменшення ризику: підвищте рівень безпеки, захистивши привілейований доступ від входу до підвищення привілеїв, і завчасно усує загрози, пов’язані з ідентифікацією, і неправильним налаштуванням.

Простіше відповідати вимогам: адаптивний контроль авторизації та уніфікований аудит спрощують виконання та демонстрацію вимог відповідності.

Централізація контролю: управляє привілейованим доступом до спільних облікових даних і всіх ідентифікацій, що охоплюють дані, програми, хмару та традиційну інфраструктуру.

Масштабуйте свою програму PAM. Використовуйте захищену хмарну архітектуру Delinea, щоб розвивати свою організацію завдяки безперебійному застосуванню контролю привілеїв і спільних можливостей.

Швидка окупність інвестицій: скористайтеся перевагами налаштування, конфігурації та робочих процесів, керованих майстром, які легко адаптувати.

Скористайтеся перевагами хмарної відмовостійкості: відчуйте найбільш стійке рішення, яке може похвалитися часом безвідмовної роботи 99,99%.

Однак якщо основні компоненти інфраструктури, які інтегруються хмарною архітектурою, не можуть задовольнити потреби в масштабованості, гнучкості та

резервуванні, тоді системи організації не такі стійка. Нехмарні компоненти можуть створювати перешкоди та сповільнювати роботу. Ці компоненти можуть створювати вразливості, які можуть відкрити двері для кібератак. Найважливіше те, що вони збільшують вірогідність і обсяг простоїв ваших критичних IT-систем і бізнес-операцій.

Щоб захистити вашу організацію від збоїв, хмарні архітектори повинні створити міцну та надійну архітектуру, яка може протистояти викликам і підтримувати потреби бізнесу рис.2.2.

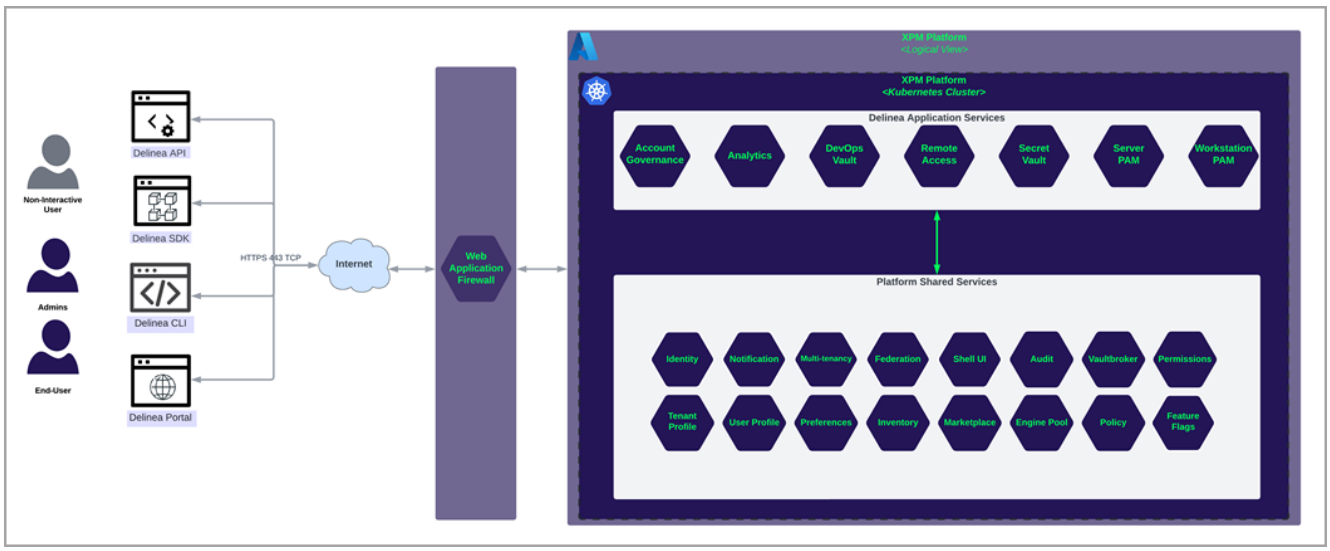

Рис. 2.2. Архітектура Delinea PAM

Архітектуру Delinea PAM розбито на понад 70 різних сервісів. Кожен із сервісів повністю ізольований і незалежний від інших сервісів. У цій моделі, якщо одна з цих служб виходить з ладу, інші служби продовжують працювати.

Розглянемо основні компненти Delinea PAM.

1. Секретний сервер

Секретний сервер (Delinea Secret Server) — це комплексний привілейований доступ рішення для керування (PAM), розроблене для захисту, контролю та керування привілейованими обліковими записами та обліковими даними в організації. Він пропонує безпечне централізоване сховище для зберігання

конфіденційної інформації, такої як паролі, ключі та сертифікати, гарантуючи, що доступ до цих критичних активів надається лише авторизованому персоналу.

Secret Server — це потужний передовий продукт із широким спектром можливостей. Незважаючи на це, його дуже легко використовувати для звичайних повсякденних операцій для нетехнічних людей.

Секрети — це пакети конфіденційної інформації з індивідуальними назвами, наприклад паролі. Секрети стосуються широкого спектру захищених даних, кожен тип представлений і створений секретним шаблоном , який визначає параметри всіх секретів на його основі. Секрети дуже потужні та надають багато способів контролю та захисту своїх даних, наприклад:

– Переконайтеся, що паролі довгі, складні та часто змінюються.

– Звільнення користувачів від необхідності запам’ятовувати численні складні паролі або коли їх потрібно змінювати. Вам потрібно лише запам'ятати свій пароль для доступу до Secret Server . Усі ваші секретні паролі керуються за вас.

– Автоматична зміна паролів через задані проміжки часу без втручання користувача.

– Визначення того, хто має доступ до секрету.

– Переконайтеся, що особа, яка має доступ до секретного сервера чи секрету, це дійсно ви.

– Запис того, хто насправді отримав доступ до секрету.

– Уся секретна інформація полів для введення тексту надійно шифрується перед збереженням у базі даних, включаючи детальний контрольний журнал для доступу та історії.

Основні функції до секретів включають:

– Перегляд секретів (включає перевірку терміну дії та історії)

– Створення секретів

– Секретні параметри конфігурації

– Редагування секретів (включає зміну паролів вручну, замість очікування закінчення терміну дії)

– Деактивація та повторна активація секретів

2. Менеджер життєвого циклу облікового запису - дозволяє знаходити, захищати, створювати та виводити з експлуатації облікові записи служби.

Аналітика привілейованої поведінки - дозволяє виявляти аномалії в поведінці привілейованого облікового запису.

Менеджер привілеїв - управляє привілеями робочої станції та контроль додатків.

3. Сервер PAM - керує ідентифікаторами та політиками на серверах.

2.4. Опис функцій компонентів рішення Delinea PAM

До основних функцій Delinea Secret Server відноситься:

Безпечне зберігання паролів: *Secret Server* зберігає привілейовані облікові дані в зашифрованому форматі, захищаючи конфіденційну інформацію від несанкціонованого доступу.

Контроль доступу: Secret Server реалізує контроль доступу на основі ролей, дозволяючи адміністраторам встановлювати дозволи та контролювати, хто має доступ до конфіденційної інформації.

Керування підвищенням привілеїв: Secret Server інтегрується з системами Windows, щоб забезпечити керування підвищенням привілеїв, допомагаючи зменшити ризик порушення даних.

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

Автоматичне керування паролями: Secret Server підтримує автоматичне керування паролями, допомагаючи оптимізувати процес керування паролями та зменшити ризик помилок, зроблених вручну.

Багатофакторна автентифікація: Secret Server підтримує багатофакторну автентифікацію, допомагаючи покращити безпеку конфіденційної інформації.

Інтеграція з іншими інструментами: Secret Server інтегрується з багатьма іншими інструментами, включаючи Active Directory, Microsoft Azure та хмарні програми, що полегшує організаціям керування своїми паролями та контролем доступу.

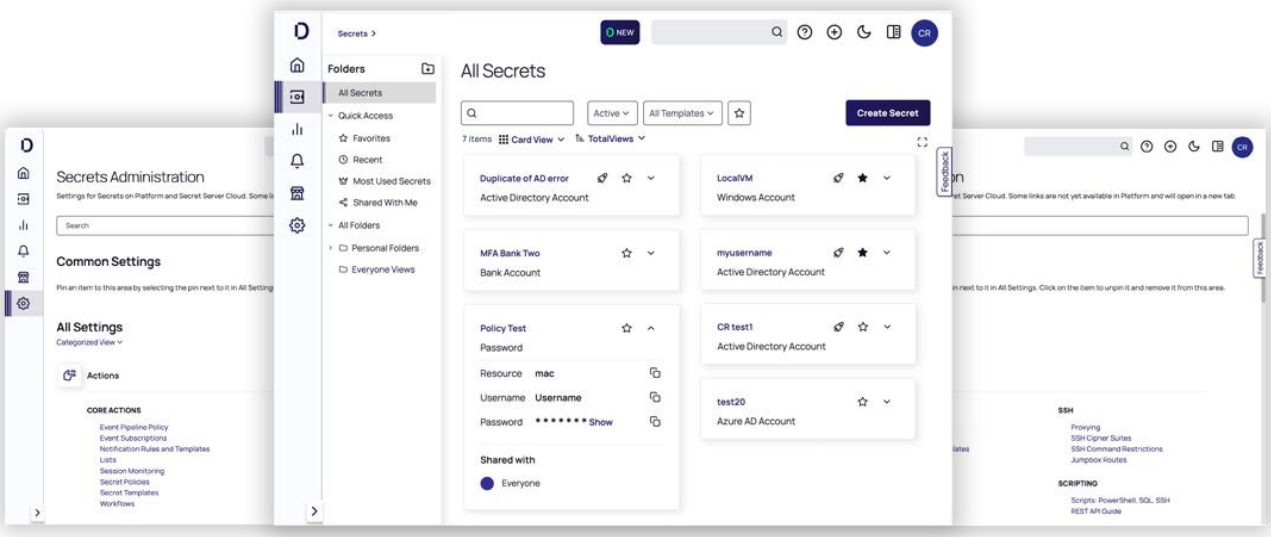

Рис. 2.3. Секретний сервер [4, 6]

Менеджер привілеїв надає наступні функції [6]:

Можливість розгорнути одного агента. Це дозволяє знаходити програми з правами адміністратора навіть на комп’ютерах поза доменом і застосовувати політики.

Визначати гнучку політику. Надає можливість підвищувати, дозволяти, забороняти та обмежувати програми лише кількома командами за допомогою майстра політики. Легке створення перших політик за допомогою The Workstation Policy Framework.

Управління/вилучення прав локального адміністратора. Створює правила для постійного визначення членства в локальній групі та автоматичної ротації привілейованих облікових даних.

Застосовувати програми. Дозволяє довіреним програмам запускати, блокувати інші або використовувати їх у ізольованому середовищі, зберігаючи модель найменших привілеїв.

Підвищити продуктивності IT і кінцевих користувачів. Дані служби підтримки зменшуються завдяки автоматизованим масовим або повторюваним операціям; люди автоматично отримують доступ до потрібних програм і систем.

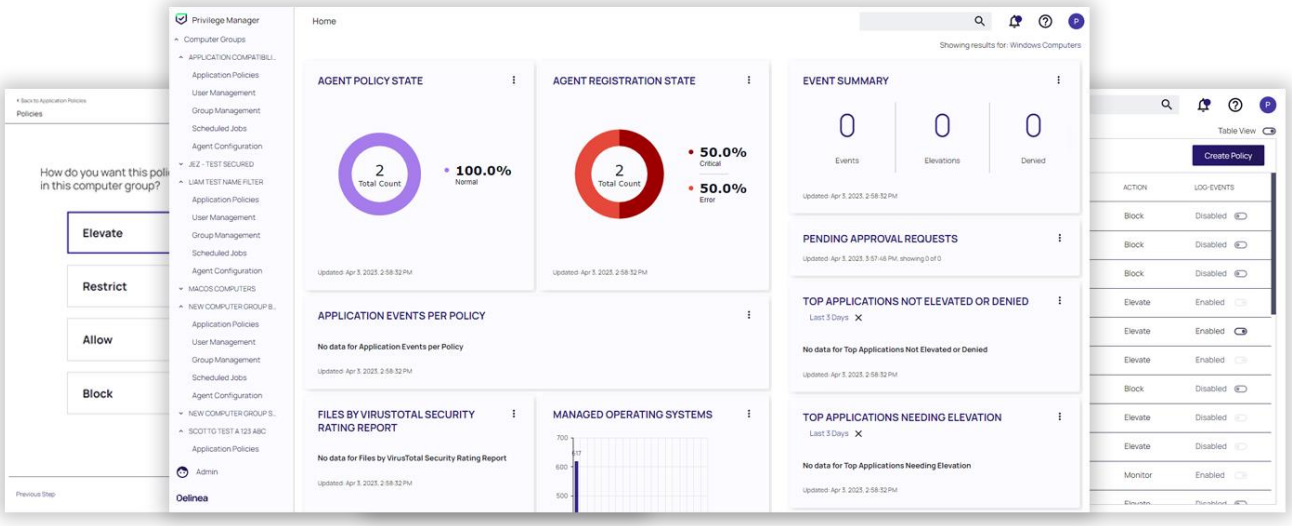

Рис.2.4. Панель менеджеру привілеїв [6]

Менеджер життєвого циклу облікового запису такі основні функції [4, 6]:

Знаходити приховані облікові записи. Це дозволяє знайти та ідентифікувати облікові записи служби.

Встановлювати робочі процеси, в основу яких покладено делегування право власності за допомогою дозволів на основі ролей.

Налаштовувати облікові записи автоматично.

Забезпечує управління на основі встановлення права власності та відповідальність за облікові записи.

Видаляти облікові записи без збоїв.

Сервер PAM виконує наступні функції:

Централізовано керує політиками входу, виконання та MFA в Active Directory (AD) (запатентовані зони) або від постачальників хмарних ідентифікаторів.

Мінімізує ризик за на основі нормативних актів і найкращих практик, таких як «нульова довіра» та «нульові постійні привілеї», щоб захистити від програм-вимагачів і атак зловживання даними.

Застосувати найменші привілеї на основі контролю доступу на основі ролей (RBAC) на рівні хоста для детального контролю та підвищення привілеїв.

Застосувати адаптивний MFA. Політики MFA застосовуються під час входу та виконання програми в Windows і Linux для більшої надійності ідентифікації та вимог страхування кіберризиків.

Покращення безпеки та відповідності. Аудиторські журнали та записи сеансів для перевірки безпеки, реагування на інциденти, відповідності та повної відповідальності.

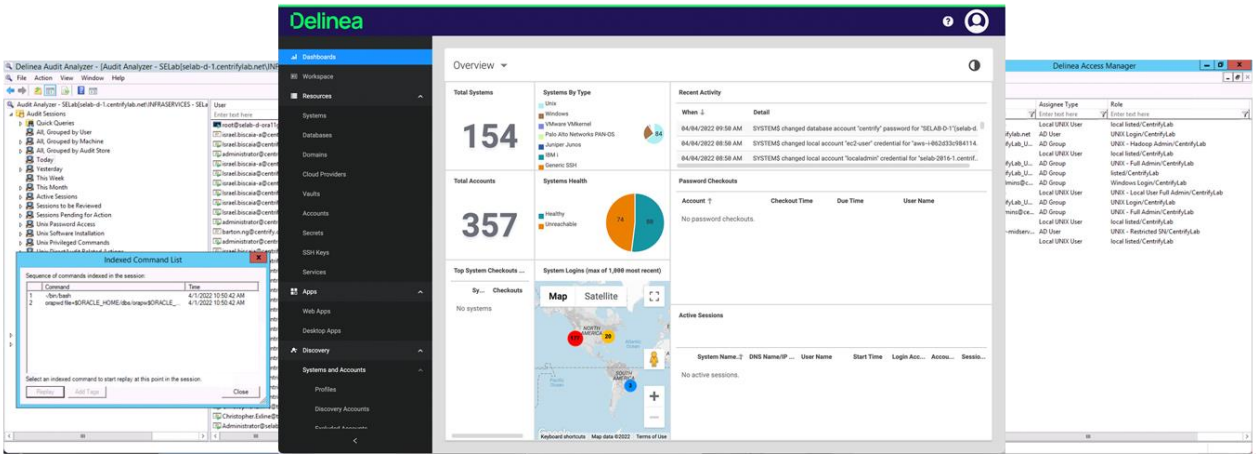

Рис. 2.5. Панель серверу PAM

За допомогою аналітика привілейованої поведінки за допомогою платформи PAM фахівці з кібербезпеки можуть виявляйте аномалії в привілейованих облікових записах в інформаційній системі організації.

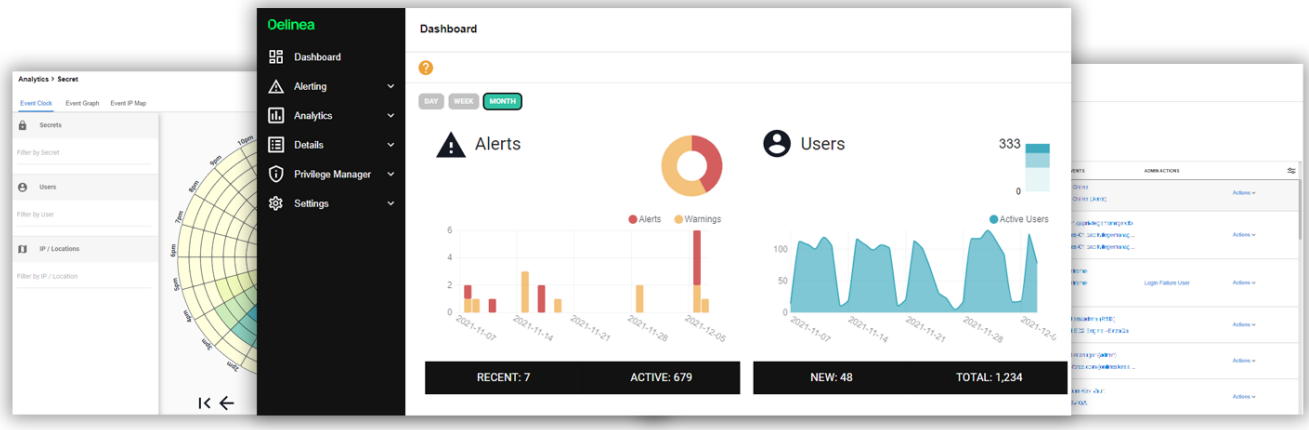

Рис. 2.6. Панель аналітики привілейованої поведінки

Аналітика привілейованої поведінки Analytics використовує розширене машинне навчання для аналізу активності привілейованих облікових записів у режимі реального часу, щоб виявити аномалії та забезпечити оцінку загроз і настроювані сповіщення.

Розширене машинне навчання аналізує всю активність привілейованого облікового запису, щоб ви могли виявляти проблеми та вимірювати ступінь порушення.

Висновки до розділу 2

1. Показано план і етапи впровадження PAM платформи, яке надає краще розуміння необхідності застосування управління привілейованим доступом.

2. Проаналізовано життєвий цикл PAM, в результаті чого визначено основні дії щодо до захисту та забезпечення привілейованого доступу.

3. Проаналізовано архітектуру платформи Delinea PAM, що дозволить підвищити стійкість організацій до загроз.

4. Визначено основні компоненти та описано основні функції платформи PAM.

3 РОЗРОБЛЕННЯ ВАРІАНТА РОЗГОРТАННЯ РІШЕННЯ PAM ПЛАТФОРМИ DELINEA УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ

3.1. Розроблення варіанта розгортання компонентів PAM платформи

Основним компонентом PAM платформи є Secret Server — це комплексне рішення для керування привілейованим доступом (PAM), призначене для захисту, контролю та керування привілейованими обліковими записами та обліковими даними в організації. Він пропонує безпечне централізоване сховище для зберігання конфіденційної інформації, такої як паролі, ключі та сертифікати, гарантуючи, що доступ до цих критичних активів надається лише авторизованому персоналу. [9]

Залежно від того, як ваші адміністратори налаштували секретний серве , ви можете увійти або за допомогою свого облікового запису Active Directory, або локального облікового запису.

Секрети — це пакети конфіденційної інформації з індивідуальними назвами, наприклад паролі. Секрети стосуються широкого спектру захищених даних, кожен тип представлений і створений секретним шаблоном , який визначає параметри всіх секретів на його основі. Секрети дуже потужні та надають багато способів контролю та захисту своїх даних, наприклад:

Переконайтеся, що паролі довгі, складні та часто змінюються.

Звільнення користувачів від необхідності запам’ятовувати численні складні паролі або коли їх потрібно змінювати. Вам потрібно лише запам'ятати свій пароль для доступу до Secret Server . Усі ваші секретні паролі керуються за вас.

Автоматична зміна паролів через задані проміжки часу без втручання користувача.

Визначення того, хто має доступ до секрету.

Переконайтеся, що особа, яка має доступ до секретного сервера чи секрету, це дійсно ви.

Запис того, хто насправді отримав доступ до секрету.

Уся секретна інформація полів для введення тексту надійно шифрується перед збереженням у базі даних, включаючи детальний контрольний журнал для доступу та історії.

До основних відомостей про секрети відноситься:

- перегляд секретів (включає перевірку терміну дії та історії)й;
- створення секретів;
- секретні параметри конфігурації;
- редагування секретів (включає зміну паролів вручну, замість очікування закінчення терміну дії);
- деактивація та повторна активація секретів.

Створена за механізмом керування доступом на основі ролей (RBAC), безпека на основі ролей (RBS) є методом Secret Server для регулювання дозволу на доступ до системи. Кожному користувачеві та групі має бути призначена роль. Secret Server постачається з трьома ролями: адміністратор, користувач і користувач лише для читання. Кожна роль містить різні дозволи, які відповідають посадовій функції користувача. За допомогою RBS забезпечується суворий детальний доступ до Secret Server.

Ролі можна призначити декілька дозволів. Наприклад, ви можете призначити ролі права адміністрування користувачів, редагування секрету, власного секрету та перегляду Active Directory. Потім цю роль можна призначити користувачу або групі.

Базова схема та конфігурація Secret Server показано на рис 3.1 :

- Додавання ліцензій
- Основні налаштування безпеки
- Налаштування автоматичного резервного копіювання
    - Heartbeat
    - Налаштування доступу для локальних і AD користувачів.

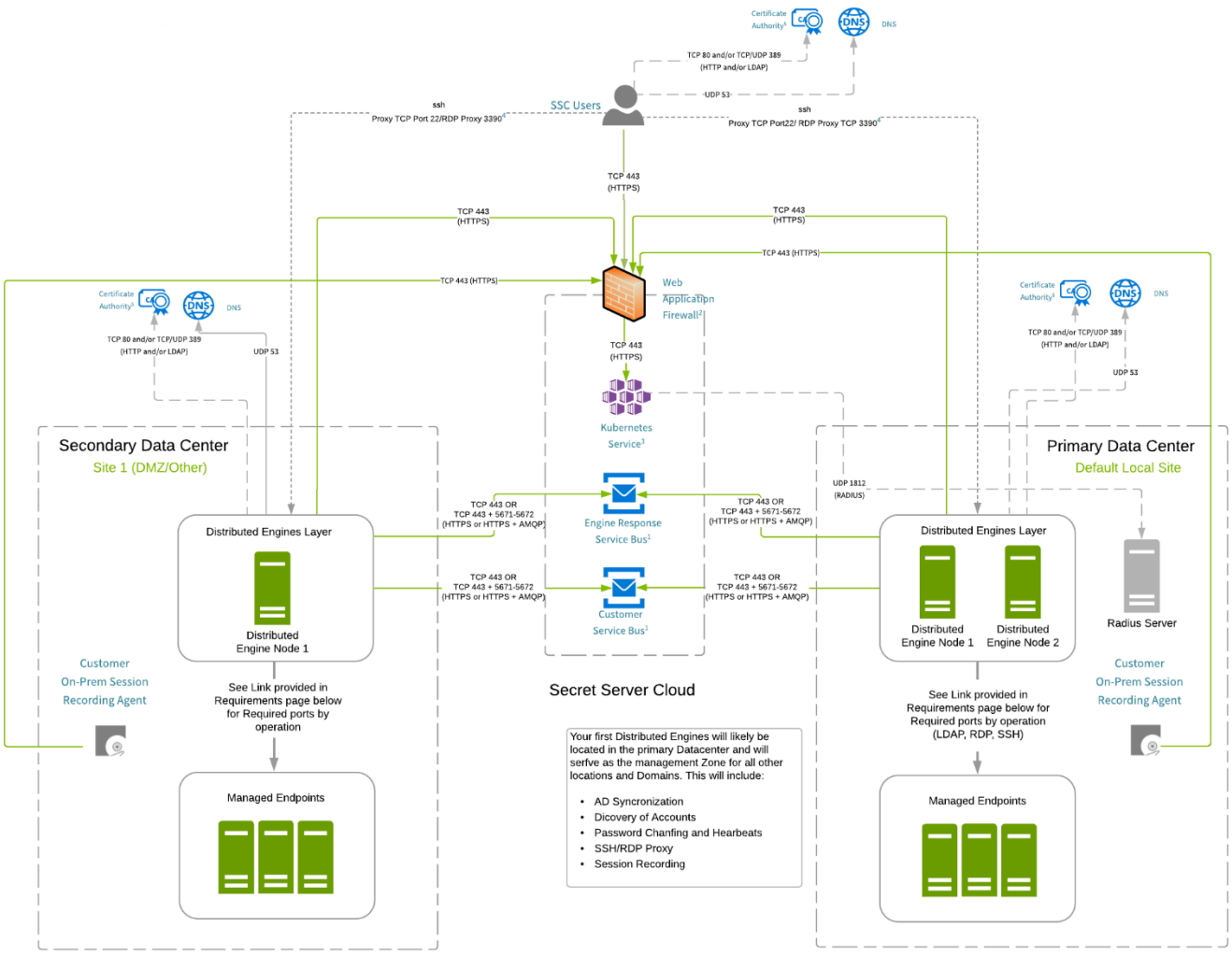

Рис.3.1. Схема розгортання серверу секретів [9]

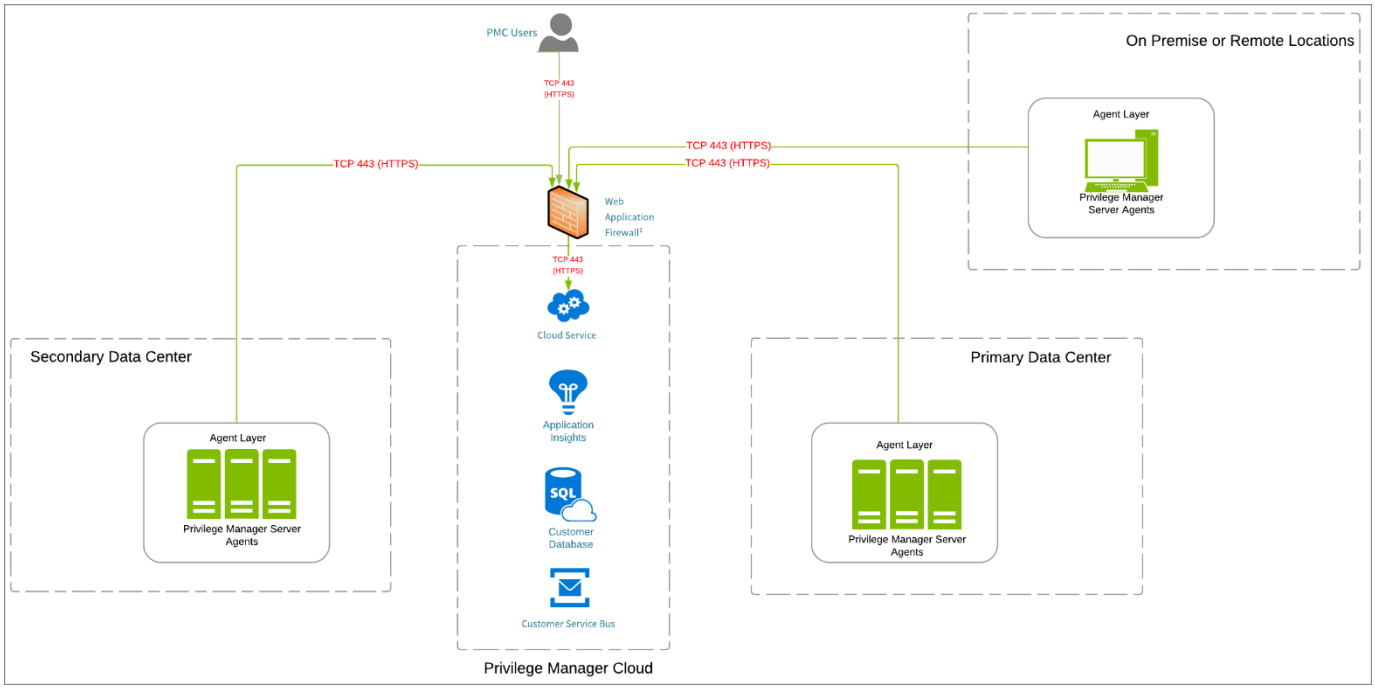

Рис. 3.2. Схема розгортання менеджеру паролів [9]

Базовий запис сеансу є ліцензованою функцією Secret Server . Він налаштований на клієнтських машинах через засіб запуску Secret Server. За допомогою програми запуску Secret Server робить посекундні знімки екрана на клієнтській машині під час записаного сеансу користувача. Ці зображення екрана користувача компілюються у відео, яке можна завантажити та відтворити з метою аудиту та безпеки. Діяльність, записана під час сеансу, базується лише на змінах екрана.

Моніторинг сеансів дозволяє адміністраторам із дозволом на моніторинг сеансів переглядати всі активні запущені сеанси в межах Secret Server. Якщо запис сеансу ввімкнено на секреті, адміністратор може спостерігати за сеансом користувача в режимі реального часу.

Адміністратори можуть здійснювати пошук сеансів серед активних і завершених сеансів. Для перегляду та пошуку сеансів перейдіть до вкладки *Адміністратора > Моніторинг сеансів* .

ПЕРЕЛІК ПОСИЛАНЬ

1. Призначення PAM URL: https://delinea.com/blog/privileged-users (дата звернення 07.03.2024).
2. Звіт Verizon. Класифікація інцидентів URL: https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/ (дата звернення 18.03.2024).).
3. Jones, C. (2023). Discover the top ten best privileged access management solutions. URL: https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions (дата звернення 28.03.2024).
4. Staff, V. B. Report: Privileged access management still absent in 80% of organizations. VentureBeat. URL: https://venturebeat.com/business/report-privileged-access-management-still-absent-in-80-of-organizations (дата звернення 05.04.2024).
5. Delinea Inc. (2023, November 11). URL: https://delinea.com/blog/privileged-access-management-lifecycle-path-to-maturity (дата звернення 16.04.2024).
6. Privileged Access Management For Dummies®, Delinea Special Edition URL: https://delinea.com/hubfs/Delinea/ebooks/delinea-ebook-privileged-access-management-for-dummies.pdf (дата звернення 21.04.2023).
7. Privilege Manager URL: https://delinea.com/products/privilege-manager (дата звернення 27.04.2024).).
8. Звіт Gartner; Магічний квадрант управління привілейованим доступом URL : https://www.gartner.com/doc/reprints?id=1-26UE4193&ct=210719&st=sb]/ (дата звернення 04.05.2024).
9. Morey J. Haber, Darran Roll Identity Attack Vectors: Implementing an Effective Identity and Access. - 2020. 200p.
10. Secret Server Documentation URL: https://docs.delinea.com/online-help/secret-server/start.htm (дата звернення 06.05.2024).

11. Introduction to Account Lifecycle Manager. URL: https://docs.delinea.com/online-help/account-lifecycle-manager/start.htm (дата звернення 07.05.2024).

12. Privileged Behavior Analytics URL: https://docs.delinea.com/online-help/privileged-behavior-analytics/start.htm#WelcometoPrivilegedBehaviorAnalyticsTechnicalAssistance (дата звернення 08.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)