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

**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія управління привілейованим доступом користувачів інформаційної системи організації на базі One Identity Safeguard»**

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*
_____ Антон МАЗУР
*(підпис)*

Виконав: здобувач вищої освіти групи БСДМ-62
Мазур АНТОН
*(прізвище, ім'я)*

Керівник к.держ.у. СКИБУН Олександр
*(науковий ступінь, вчене звання, прізвище, ім'я)*

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

Київ 2025

**ЗМІСТ**

**Стор.**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

COBIT - Control Objectives for Information and Related Technology

NIST - Національний інститут стандартів і технологій США

PAM - Privileged Account Management

PASM - Privileged account and session managemen

PEDM - Privilege elevation and delegation management

PSM - Privileged session management

SM - Secrets management

SoD - Separation of Duties

SRM- security and risk management

СКПП — система контролю привілейованих користувачів

# ВСТУП

*Актуальність дослідження.*. Захист привілейованих облікових записів гостро стає при організації кіберзахисту інформаційної системи організації. Це пов'язано з тим, що організації постійно страждають від складних забезпечених ресурсами кіберзлочинців. Компрометація привілейованих облікових записів використовується в більшості з най відомих кібератак. На сьогоднішній день, існує багато заходів для зниження ризиків компроментації, або викрадення привілейованих облікових засобів, а отже і привілейованих користувачів . Відносно прості поліпшення процесів і регламентів в поєднанні з технологією управління привілейованим доступом, які пов'язані з управлінням сесіями та використанням розширеної аналітики, можуть допомогти фахівцям виявляти скомпрометовані привілейовані облікові записи і зупинити атаку зловмисників, перш ніж вони завдадуть шкоди організації.

Таким чином необхідно застосовувати методи та засоби захисту привілейованих користувачів інформаційної системи організації. Такі методи та засоби дозволять захистити привілейовані облікові записи користувачів інформаційної системи організації. Отже, наведені аргументи актуалізують дослідження технології управління привілейованими користувачами облікових записів інформаційної системи організації.

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

*Предмет дослідження* – технологія управління привілейованим доступом інформаційної системи організації.

*Метою роботи* – є розробка варіанту технології управління привілейованим доступом користувачів інформаційної системи організації та розробка рекомендації щодо її застосування.

Наукові завдання:

Провести аналіз проблеми управління привілейованим доступом інформаційної системи організації;

проаналізувати основні загрози та підходи управління привілейованим доступом інформаційної системи організації;

дослідити методи та засоби управління привілейованим доступом інформаційної системи організації;

розробити варіант технології управління користувачами привілейованого доступу інформаційної системи організації на базі One Identity Safeguard.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту привілейованих даних користувачів інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці варіанту налаштування модуля Safeguard for Privileged Passwords технології One Identity Safeguard щодо управління привілейованих доступом інформаційної системи організації, а також у розробці рекомендацій щодо використання даної технології в метою виявлення порушень привілеїв інформаційної системи організації.

*Апробація результатів.*

Петухова М.О., Мазур А.Т. Технологія управління привілейованим доступом: порівняння рішень. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С. 21-23.

# 1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ДАНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

## 1.1.Аналіз необхідності застосування привілейованого доступу інформаційної системи організації

Управління привілейованим доступом (PAM) - це технологія, яка використовується для захисту, контролю та моніторингу віддаленого доступу до активів організації. Вона орієнтована на привілейованих користувачів, оскільки їхні облікові записи зазвичай мають найвищий рівень доступу, який у чужих руках може становити значну загрозу для важливих для бізнесу даних. Рішення PAM призначені для забезпечення доступу лише авторизованого персоналу до будь-яких систем, програм та даних, які визнані важливими для компанії.

Привілейовані облікові записи належать співробітникам, які мають багато прав у системі — змінювати важливі налаштування, роздавати доступи іншим співробітникам, створювати та правити важливі документи. Вони належать керівникам відділів, системним адміністраторам, офіцерам безпеки, генеральному директору та його заступникам.

Рішення управління привілейованим доступом (PAM - Privileged Access Management) – надають інструменти, необхідні для моніторингу та звітування про стан безпеки в організаціях. Найнадійніші системи PAM можна використовувати для виконання кількох нормативних вимог, не порушуючи щоденну діяльність користувачів і адміністраторів.

Рішення PAM дозволяє заощаджувати час і гроші, спрощуючи аудит і дотримання вимог щодо конфіденційності та безпеки, передбачених різними законами, постановами та стандартами, такими як GDPR, ISO 27001, PCI DSS, HIPAA, SOX, FIPS, NIST [9].

Управління привілейованим доступом (PAM) визначає суть захисту привілейованих облікових записів в організаціях з різних галузей та регіонів. Програмне забезпечення PAM може оптимізувати процес, автоматично

перевіряючи привілейовані особи, обмежуючи доступ до конфіденційної інформації та обмежуючи здатність зловмисників переміщатися у вашому IT-середовищі.

Ефективне керування привілеями допомагає пройти перевірку відповідності та зменшити кібер ризик.

Окремі компоненти PAM надають різні переваги IT-інфраструктурі компанії та допомагають адміністраторам полегшити роботу. Хоча нормативні вимоги вимагають багато параметрів, PAM допомагає виконати їх за замовчуванням. Основними серед них є:

PAM надає всі необхідні відомості (за допомогою функції запису сеансу) для завершення будь-якого розслідування порушення

PAM допомагає централізовано контролювати всі адміністративні завдання

PAM допомагає у всебічному аудиті організацій, щоб легко відповідати вимогам

Розгортання рішення PAM запобігає будь-якому несанкціонованому доступу організацій до привілейованих облікових записів (з детальним контролем доступу)

Рішення PAM ідентифікує привілейованих користувачів перед входом в облікові записи, що опосередковано допомагає виявляти підозрілих користувачів

PAM навіть допомагає адміністраторам виявляти будь-які підозрілі дії в IT-середовищі за допомогою моніторингу в реальному часі через інформаційну панель адміністратора

PAM оптимізує загальну безпеку та посилює захист даних

Як згадувалося, PAM може допомогти організаціям відповідати численним стандартам безпеки. Наприклад, PAM можна впровадити як прямо, так і опосередковано для підтримки зусиль щодо відповідності GDPR та ISO/IEC 27001:2013:

- Посилення доступу до критичних даних;
- Надання адміністраторам повної видимості дій користувачів;
- Допомога у визначенні та застосуванні ретельної політики безпеки;
- Запис і реєстрація всіх дій внутрішніх і зовнішніх сторін;

– Дозволяє адміністраторам визначати спеціальні правила доступу для кожного користувача;

– Інтеграція з більшою екосистемою кібербезпеки для надійної безпеки;

– Створення точної інформації про сеанси привілейованого облікового запису.

*Загальний регламент захисту даних Європейського Союзу (GDPR)*

Відповідність GDPR ЄС вимагається від будь-якої компанії, яка має справу з особистою інформацією будь-якого громадянина Європейського Союзу, що дозволяє ідентифікувати особу. Сертифікація GDPR присвячена роботі з персональними даними, а доступ до сенситивної персональної інформації можна вважати привілейованим. Аудитори особливо зацікавлені в захисті облікових даних привілейованого облікового запису, оскільки вони сприяють найбільшій кількості порушень безпеки ідентифікаційної інформації. У компанії можуть існувати сотні чи тисячі таких привілейованих облікових записів, і аудитори хочуть, щоб ці паролі регулярно змінювалися та посилювалися, щоб вони були довшими та складнішими.

Насправді, PAM вважається одним з ключових елементів для відповідності вимогам GDPR, і допомагає з пунктами:

– Випадкове або незаконне знищення, втрата, зміна або доступ до персональних даних;

– Повідомлення контролюючого органу про порушення персональних даних;

– Оцінка впливу на захист даних;

– Право на компенсацію та відповідальність.

Більша частина вимог відповідності GDPR спирається на логування доступу до персональних даних для можливості розслідування.

До відповідальності за недотримання вимог можуть бути притягнуті як компанії з території Європейського Союзу, так і компанії, які зареєстровані поза межами ЄС. Якщо Ви обробляєте персональні дані резидентів ЄС, то ваша компанія

має дотримуватися вимог GDPR і безпечна обробка та захист персональних даних повинні стати невід'ємною частиною та принципом діяльності вашої компанії [10].

*ISO 27001*

В одному з найвідоміших стандартів ISO 27001 темі PAM присвячений пункт A 9.2.3: Management of privileged access rights: The allocation and use of privileged access rights should be restricted and controlled (Керування правами привілейованого доступу: видача та використання прав привілейованого доступу має бути обмеженj. та контрольованj.). При поглибленні в гайд по імплементації можемо побачити вимоги більш детально. Привілейовані облікові записи та користувачі, яким потрібен до них доступ повинні бути ідентифіковані, дозволи повинні видаватись за потреби або за умови, необхідність авторизації перед отриманням привілейованого доступу, необхідність визначеного терміну дії для паролів від привілейованих акаунтів. Також згадується видалення користувачів з груп локальних та доменних адміністраторів, з формулюванням "Звична активність не може виконуватись з привілейованого ID" [10].

Також PAM допомагає з пунктом A.9.4.4: Використання привілейованих службових програм і неявно згадується в інших частинах стандарту:

Привілейовані права доступу, пов'язані з кожною системою чи процесом, наприклад, операційна система, система керування базами даних і кожна програма, а також користувачі, яким вони повинні бути призначені, повинні бути ідентифіковані [10].

Привілейовані права доступу повинні надаватися користувачам на основі потреби у використанні та на основі подій за подіями відповідно до політики контролю доступу, тобто на основі мінімальних вимог до їхніх функціональних ролей [10].

Слід підтримувати процес авторизації та запис усіх наданих привілеїв. Привілейовані права доступу не повинні надаватися до завершення процесу авторизації [10].

Необхідно визначити вимоги щодо закінчення терміну дії привілейованих прав доступу [10].

Привілейовані права доступу мають бути призначені ідентифікатору користувача, відмінному від тих, які використовуються для звичайної комерційної діяльності. Звичайна бізнес-діяльність не повинна здійснюватися з привілейованих ідентифікаторів [10].

Компетенції користувачів із привілейованими правами доступу слід регулярно переглядати, щоб перевірити, чи відповідають вони своїм обов'язкам.

Необхідно встановити та підтримувати спеціальні процедури, щоб уникнути несанкціонованого використання загальних ідентифікаторів користувачів адміністрування відповідно до можливостей конфігурації системи [10].

Для загальних адміністративних ідентифікаторів користувачів слід підтримувати конфіденційність секретної інформації автентифікації під час спільного використання (наприклад, змінювати паролі часто та якнайшвидше, коли привілейований користувач залишає або змінює роботу, повідомляючи їх між привілейованими користувачами за допомогою відповідних механізмів) [10].

*Payment Card Industry Data Security Standard (PCI DSS)*

Ще одним відомим стандартом є PCI DSS, з яким також може допомогти рішення PAM. Вимога 2 забороняє використання дефолтних паролей, Вимога 7 визначає необхідність контролю доступу до персональної інформації володаря картки, Вимога 8 потребує ідентифікацію та автентифікацію для доступу до критичних систем. Остання також вимагає можливість зворотного пошуку, хто саме отримав доступ до даних. І 10 вимога становить, що весь доступ до мережевих ресурсів та інформацію про картки має бути записаний [11].

Системи PAM працюють як поєднання технологій та найкращих практик для управління привілейованим доступом в IT-інфраструктурі організації [11]. Є кілька важливих особливостей PAM, які слід зазначити:

контроль доступу,

управляння паролями,

управління привілейованими сесіями,

аудит та звітність,

забезпечення відповідності.

Основними ключовими функціями PAM є інструменти контролю доступу. Вони гарантують, що лише авторизовані користувачі можуть отримати доступ до привілейованих облікових записів та даних. Відповідно до підходу *Zero Trust,* рішення PAM гарантують, що користувачі отримують доступ до певних додатків та облікових записів тільки за необхідності та з певної причини. Адміністратори можуть визначати та планувати доступність ресурсів для користувачів та відповідним чином контролювати їх.

Наступна згадана ключова функція – управляння паролями. Рішення PAM допомагають запровадити суворі політики паролів для привілейованих облікових записів. Засоби управляння паролями забезпечують унікальність, складність та регулярну зміну привілейованих паролів для запобігання несанкціонованому доступу. Це важливо сьогодні, коли вкрадені або скомпрометовані облікові дані є одним з найпоширеніших векторів початкової атаки під час витоку даних.

Інструменти управління привілейованими сесіями дозволяють організаціям записувати та проводити аудит привілейованих сесій, що допомагає виявити та розслідувати будь-яку підозрілу активність. Деякі рішення PAM забезпечують взаємодію в реальному часі під час сеансів користувачів, дозволяючи адміністраторам приєднуватись, розділяти, зупиняти або завершувати потенційно підозрілі сеанси одразу після виявлення будь-якого прояву небезпечної поведінки. Цей підхід здебільшого спрямований проти інсайдерських загроз, які стають дедалі більш поширеними. Шкідливий інсайдер – це, як правило, нинішній чи колишній

співробітник чи діловий партнер, який має привілейований доступ до конфіденційних даних чи критично важливої інфраструктури компанії.

Описуючи PAM, не можна не згадати про функції аудиту та звітності, які також відіграють ключову роль у забезпеченні безпеки. Функції запису та резервного копіювання сеансів дозволяють згодом проаналізувати події та визначити об'єкти чи осіб, відповідальних за порушення процедур безпеки. Рішення PAM надають інструменти, які дають змогу співробітникам служби безпеки шукати відповідні ключові слова, пов'язані з інцидентом, під час підозрілих сесій. Коли відбувається витік даних, компанія має можливість просканувати будь-які сліди чи докази злочину.

Сучасні PAM-системи можуть запропонувати цілу низку унікальних рішень. Запобігання за допомогою штучного інтелекту – одна з найбільш передових функцій на ринку. ШІ аналізує та створює схеми поведінки індивідуально для кожного користувача. Про будь-яку підозрілу активність негайно повідомляється адміністратору, тому він може легко відстежити та звузити коло потенційних загроз, знищити їх та притягнути певного суб'єкта до відповідальності за його дії.

PAM зазвичай включає три основні компоненти: менеджер доступу, менеджер сеансів, менеджер паролів.

*Менеджер доступу:* Менеджер доступу допомагає групам безпеки керувати всім доступом користувачів (внутрішнім, віддаленим, контрактним тощо) через єдиний портал. Незмінні журнали аудиту гарантують, що все відстежується та контролюється під час інтеграції з вашими існуючими рішеннями для бездоганної безпеки.

*Менеджер сеансів*: Менеджер сеансів відстежує та записує всі дії користувачів у реальному часі, щоб запобігти, виявити та припинити будь-які підозрілі дії. Адміністратори мають повний контроль над точними системами або даними, до яких може отримати доступ особа, і автоматично отримують сповіщення, якщо щось піде не так. Цей компонент також допомагає командам безпеки, створюючи відеозаписи всіх сеансів, які можна шукати за допомогою

технології оптичного розпізнавання символів, що значно прискорює розслідування порушень.

*Менеджер паролів*: Менеджер паролів захищає всі паролі в зашифрованому сховищі та запобігає будь-якому прямому доступу до кореневих паролів. Автоматизована регулярна зміна паролів підвищує безпеку та звільняє від такої рутинної роботи технічних спеціалістів. Це допомагає адміністраторам застосовувати сувору політику паролів для подальшого захисту організацій.

## 1.2. Призначення привілейованого доступу до інформаційних систем та переваги його застосування

Організації впроваджують технології управління привілейованим доступом (Privileged Account Management -PAM) [1, 2], які надають ряд переваг, а саме:

зменшення площини атаки;

пом'якшення впливу кібератаки на інформаційну систему,

підвищення продуктивності роботи аналітиків,

зниження ризиків від помилок користувача при роботі з інформаційною системою.

Головною метою впровадження PAM в інформаційну систему організації є обмеження прав доступу і дозволених дій для облікових записів, систем, пристроїв (таких, як IoT), процесів і додатків.

PAM є одним з головних механізмів забезпечення безпеки доступу до інформаційної системи і вважається багатьма аналітиками одним з найбільш важливих проектів безпеки для зниження ризиків. Адже PAM забезпечує детальний огляд, контроль і аудит над привілейованим доступом і діями [2].

Привілей в інформаційних технологіях надають повноваження, завдяки яким обліковий запис або процес працює в обчислювальній системі (Рис.1.1).

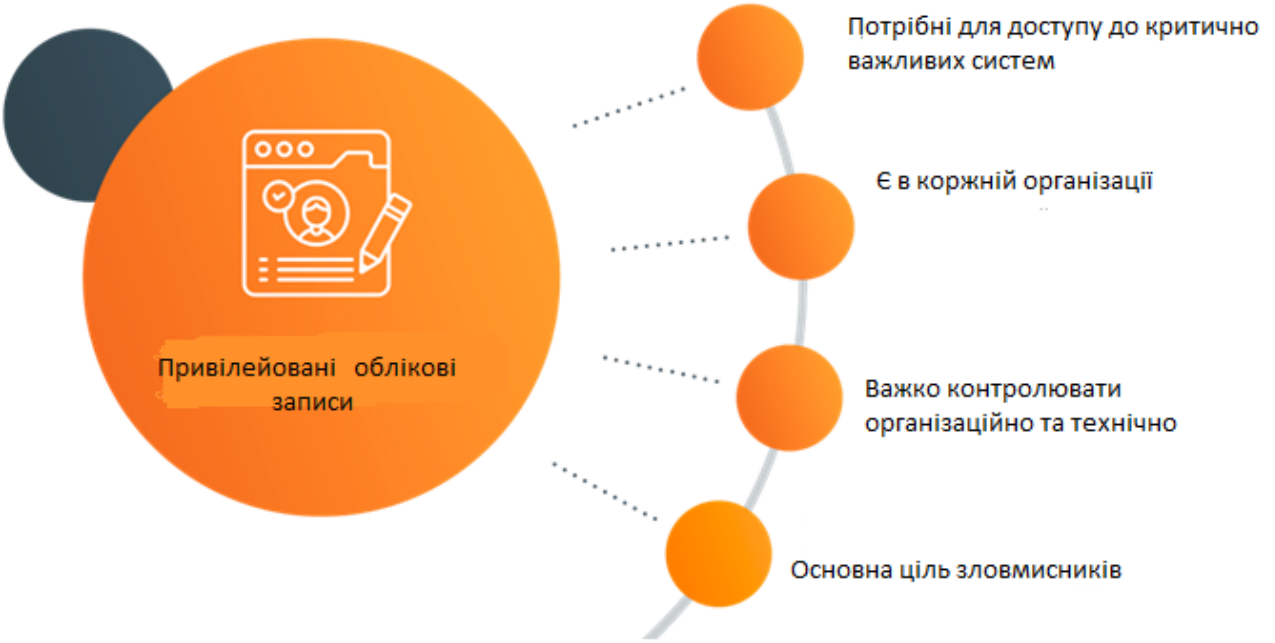


Рис.1.1. Привілейовані облікові записи

Для організацій можливо скласти типів користувачів які мають привілейований доступ, а саме:

Привілеї включають в себе дозволи на виконання таких дій:

вимикання систем;

завантаження драйверів пристроїв;

налаштування мереж або систем;

підготовка і налаштування облікових записів користувачів, додатків тощо;

підготовка і налаштуванняа хмарного доступу  тощо.

Співробітникам надаються привілеї, засновані на ролях (наприклад, маркетинг, менеджмент або IT-відділ), або на інших параметрах (стаж роботи, часу доби і т. д.).

- технічні
- системні
- для керування пристроями
- адміністратори
- розробники та DevOps-и

– програми
– бази даних
– бізнес-користувачі.

Як приклад привілейованого доступу користувачів інформаційної системи [2] можна надати такі типи користувачів, як це показано на рис. 1.2.

Локальні адміністративні облікові записи - неособисті облікові записи, що забезпечують адміністративний доступ тільки до локального хосту або примірника.

Адміністративні облікові записи домену - привілейований адміністративний доступ до всіх робочих станцій і серверів в домені.

Аварійні облікові записи - непривілейованих користувачі з адміністративним доступом до захищених систем в разі надзвичайної ситуації.

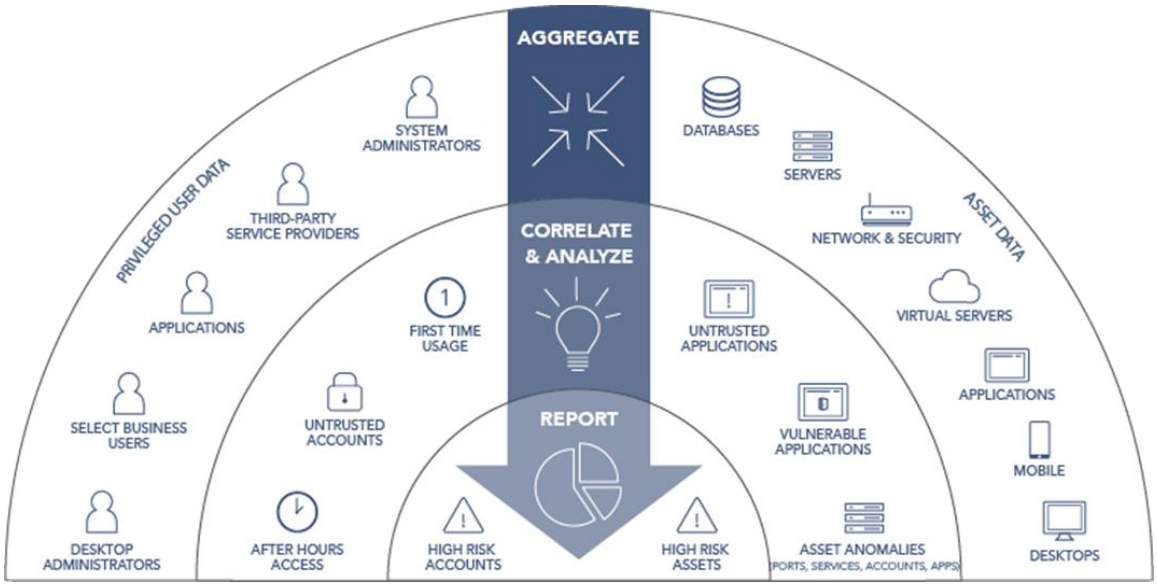


Рис.1.2. Користувачі привілейованого доступу

Сервісний акаунт - привілейований локальний або доменний обліковий запис, який використовується додатком або службою для взаємодії з операційною системою.

Облікові записи додатків - для доступу до баз даних, запуску пакетних завдань або сценаріїв або надання доступу до інших додатків.

Привілеї надають користувачам, додаткам та іншим системним процесам право доступу до певних ресурсів. Однак можливість зловживання цими привілеями, є як з боку внутрішніх, так і зовнішніх зловмисників та створює серйозну загрозу безпеці для організацій.

Основні загрози привілейованого доступу включають найпоширеніші вектори привілейованих загроз:

1. Зовнішні та внутрішні загрози: хакери, шкідливі програми.
2. Внутрішні ризики: інсайдери, партнери, помилки, спричинені користувачами.

Переваги впровадження управління привілейованим доступом (PAM)

Впровадження PAM мінімізує ризики та надає низку важливих переваг:

1. Мінімізація ризику порушення безпеки:
    a. Обмеження області порушення: Якщо порушення все ж станеться, PAM обмежує його масштаби.
    b. Зменшення площі атаки: Обмеження привілеїв для людей, процесів та програм захищає від зовнішніх і внутрішніх загроз.
    c. Демонтаж ланцюжка кібератак: PAM забезпечує захист як від зовнішніх, так і від внутрішніх атак.
2. Протидія шкідливим програмам:
    a. Багато різновидів шкідливого ПЗ потребують підвищених привілеїв для установки або запуску.
    b. Видалення надмірних привілеїв (застосування принципу найменших привілеїв) заважає шкідливому ПО закріпитися в системі.
3. Зниження експлуатаційних ризиків:
    a. Зменшується ймовірність проблем несумісності між додатками/системами.
    b. Знижується загальний ризик простоїв.
4. Спрощення аудиту. PAM допомагає створити менш складне, а отже, більш просте для аудиту середовище.

Опис схеми "Управління привілейованим доступом" (PAM)

На рис 1.3. показано типовий потік процесу Управління привілейованим доступом (PAM), який забезпечує безпечний і контрольований доступ користувачів до критично важливих ресурсів.

*Центральний потік доступу*

1. Запит доступу користувачів. Процес починається, коли користувач робить запит на отримання привілейованого доступу до певної системи чи ресурсу.

2. Правила затвердження. Запит користувача спочатку надходить до блоку "Правила затвердження". Це ключовий етап, де визначається, чи має користувач право на цей доступ, згідно з політиками безпеки.

3. Маршрутизація доступу. Після затвердження запит може бути спрямований двома шляхами:

- Відновлення пароля: Цей шлях, позначений замком, імовірно, використовується для безпечного надання або відновлення облікових даних (пароля) для привілейованого доступу.
- Проксі сесії: Це основний механізм контролю, позначений ключем. Він виступає посередником між користувачем і цільовим ресурсом, забезпечуючи, що привілейовані сесії проходять через PAM-систему.

4. Доступ до ресурсів: Зрештою, через "Проксі сесії" (який може взаємодіяти з "Відновленням пароля"), користувач отримує доступ до цільових систем, які розташовані у крайньому правому блоці:

- Сервери
- Робочі станції
- Пристрої
- Застосунки (Програми)
- Бази даних
- Медіа
- Хмара

*Контроль та Моніторинг (ЗАПИС ТА АУДИТ)*

Уся активність, пов'язана з привілейованим доступом, перебуває під постійним контролем блоку "ЗАПИС ТА АУДИТ":

Запис сесій: Ведеться повний відео- або текстовий запис дій, які виконуються під час привілейованої сесії.

Повтор сесій: Дозволяє службі безпеки відтворити записані сесії для розслідування інцидентів.

Аудит журналів: Здійснюється перевірка та аналіз системних журналів, що стосуються привілейованих дій.

Архів журналів: Забезпечує довгострокове зберігання журналів для дотримання нормативних вимог та майбутніх аудитів.


Рис.1.3. Робочий процес привілейованого управління паролями

Отже, робочий процес привілейованого доступу не просто надає доступ, а й контролює, реєструє та моніторить кожну привілейовану дію, мінімізуючи ризики зловживання.

### 1.3. Загрози та підходи до організації привілейованого доступу

За даними Centrify, зловживання привілейованими даними є основною причиною витоків даних у корпораціях. Це дослідження було отримано в результаті опитування, проведеного серед 1000 IT-керівників у США та Великій Британії. Результати були викладені в новому звіті , в якому зазначається, що «74% порушень стосувалися доступу до привілейованого облікового запису» [6].

Ця цифра також досить добре корелює з висновками Звіту про розслідування витоків даних Verizon за 2024 рік.

Було виявлено, що вражаючий 81% порушень був безпосередньо пов'язаний з паролями, які були або викраденими, або слабкими, або просто паролями за замовчуванням, які організації не змінили на безпечніші (рис.1.4).

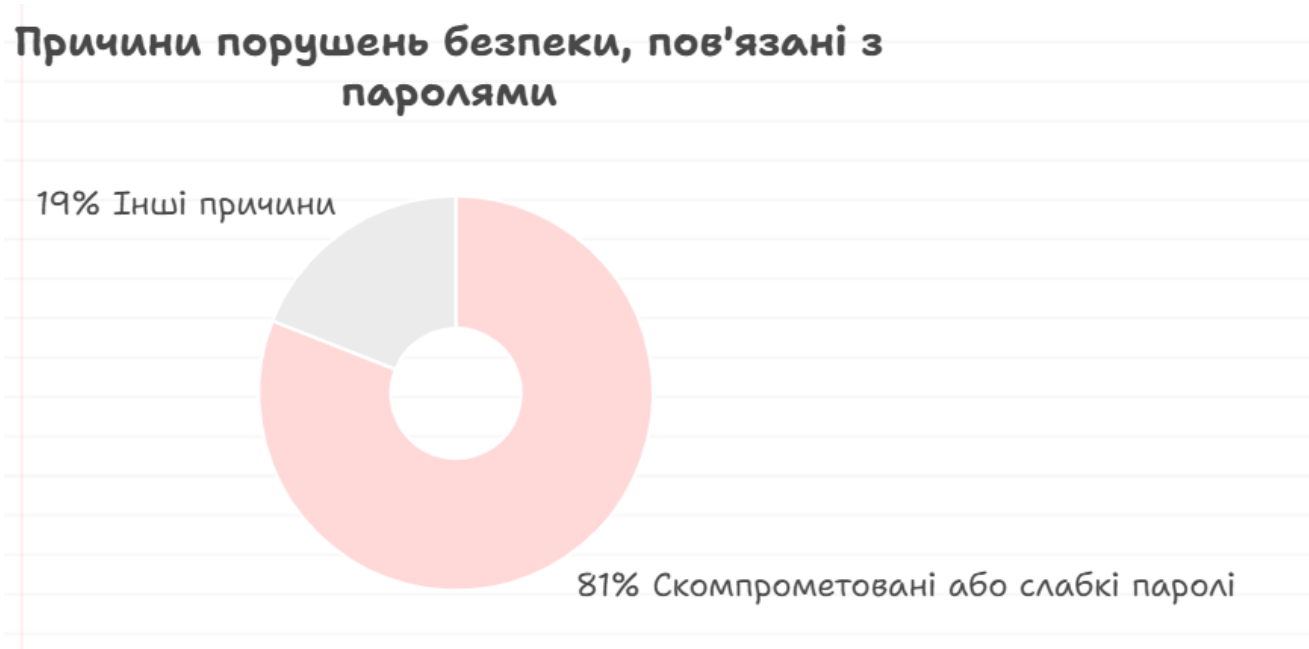


Рис.1. 4. Причини порушень привілейованого доступу

Для компаній важливо усвідомлювати, що порушення — це не лише зовнішні загрози, дуже часто вони відбуваються всередині організації.

Конфіденційність даних та захист даних йдуть пліч-о-пліч. Конфіденційність даних наразі є глобальною проблемою, і більшість організацій забезпечують дотримання нових законів і правил.

Однак багатьом організаціям також доводиться стикатися з менш розголошеними, але цілком реальними загрозами, які створює неефективна політика захисту даних. Мабуть, найочевиднішою з цих загроз є сума грошей, яку компанії можуть втратити через кожне порушення.

Дослідження «Вартість порушення безпеки даних», спонсороване IBM, показав [7], що витоки даних не лише зростають, але й стають дорожчими. Цікаво, що витоки, що відбуваються в США, як правило, мають найвищі витрати, стягуючи майже 8 мільйонів доларів для відповідної організації.

IBM зменшує цю цифру до 148 доларів за «втрачений або викрадений запис, що містить конфіденційну інформацію» [7].

Наслідки витоків даних стосуються набагато більше, ніж очевидні грошові втрати. Існує також проблема недовіри, з якою компанії можуть зіткнутися з боку поточних та потенційних клієнтів, а також з боку інвесторів та ділових партнерів.

Звіт BeyondTrust [8] про загрози привілейованого доступу за 2024 рік був складений на основі опитування понад 1000 ключових IT-фахівців з різних галузей промисловості в США, регіоні EMEA та Азіатсько-Тихоокеанського регіону. Цей дослідницький звіт, проведений спільно з незалежним дослідницьким агентством Loudhouse, детально досліджує ландшафт загроз привілейованого доступу у 2024 році, зосереджуючись на тому, як IT-фахівці вирішують питання безпеки привілейованого доступу.

На основі звіту про загрози привілейованого доступу [8], загрози розподіляються на внутрішні загрози та загрози постачальників. (рис.1.5)

Внутрішні загрози - це ризики, що виникають всередині організації, головним чином стосуються працівників:

64% респондентів вважають, що вони постраждали від порушення через неправомірне використання або зловживання доступом співробітників.

90% тих, хто має повністю інтегровані інструменти PAM (керування привілейованим доступом), впевнені, що можуть виявляти конкретні загрози від співробітників із привілейованим доступом.

46% вважають, що їхні рішення повністю інтегровані.

Загрози з боку постачальників,основна увага приділяється ризикам, що виникають через зовнішніх постачальників:

182 – це середня кількість постачальників, які щотижня входять до IT-систем . Це свідчить про великий обсяг зовнішнього доступу.

58%  вважають, що мають місце порушення, пов'язані з постачальниками.

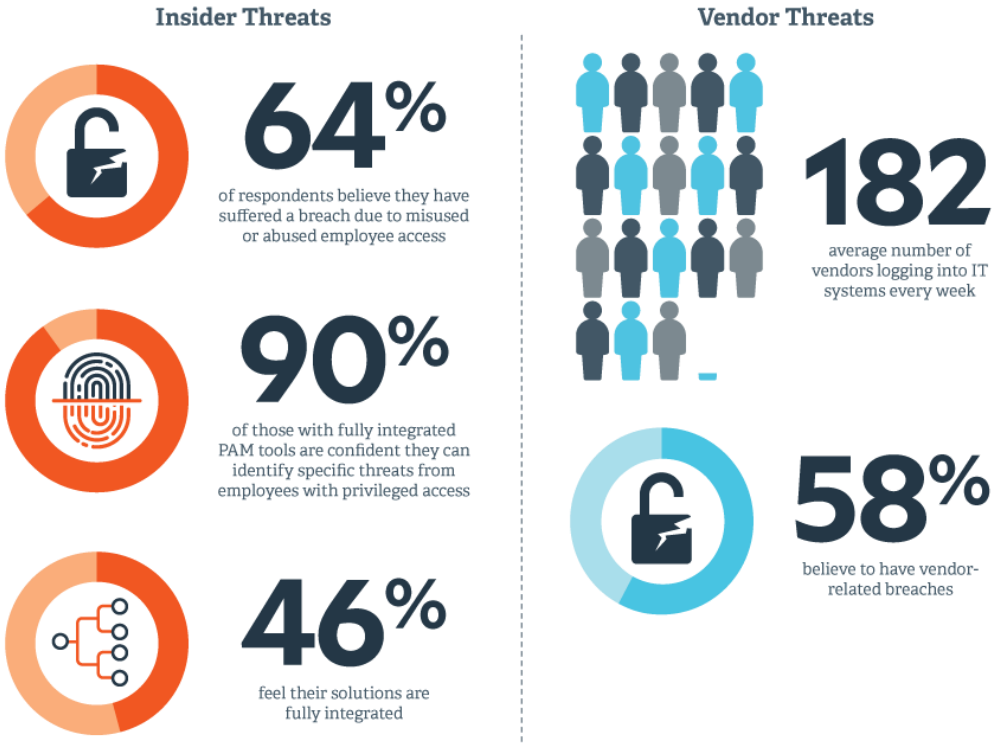


Рис.1.5. Відсоток загроз привілейованого доступу

Розглянемо питання моделювання атаки на привілейований доступ. Атаки на привілейованих користувачів, як правило на системних адміністраторів, відбуваються, але набагато частіше зловмисники вибирають більш просту початкову точку атаки. Звичайні співробітники, як правило, менш технічно

обізнані, і їх простіше почати атакувати. Як тільки облікові дані простого користувача скомпрометовані, зловмисники можуть переключити увагу на кінцеву точку атаки - привілейовані облікові записи.

Більшість атак починаються з спроби ввести воману нічого не підозрюючих користувачів. Це відбуваєтья в ході фішингової атаки, коли зловмисник за допомогою електронної пошти, месенджерів або соціальних мереж намагається переконати жертву надати конфіденційну інформацію (облікові дані), або пропонує відкрити документ, або перейти по посиланню, в результаті чого встановлює шкідливе ПЗ на комп'ютер користувача.

Як тільки зловмисники отримують доступ до IT-середовища жертви, починається стадія внутрішньої розвідки. Зловмисники спробують зібрати більше інформації про інфраструктуру організації, скласти карту мережі і систем, які туда входять. Знання про мережу допоможе зловмисникам отримати більші привілеї і досягти своєї кінцевої мети - наприклад, отримати доступ до домену. Є три основні методи, які використовуються для підвищення привілеїв –це передача хеша, перехоплення SSH-ключа, експлойти ядра і служб. Саме це дозволяє встановити повноцінний контроль над цільовою системою організації [4]. На рис.1.6 проілюстровано вектор атаки отримання привілейованого доступу за наданим прикладом.

Тож розглянемо загальні підходи для захисту та управління привілейованого доступу.

*1. Сформувати повний та актуальний список привілейованих облікових записів*

Зі зростанням IT-інфраструктури збільшується і кількість привілейованих облікових записів. Керуючи тисячами серверів та мережевих пристроїв, компаніям часто не вистачає точності в інвентаризації активів [4].

*2. Обмежити область дії кожного привілейованого облікового запису*

Потрібно використовувати принцип найменших повноважень для всіх привілейованих облікових записів: кожен обліковий запис повинен мати ті права, які необхідні для виконання конкретного завдання. Наприклад, обліковий запис для

адміністрування програми не повинен мати жодних системних привілеїв, крім необхідних для внесення змін до конфігурації програми та її перезапуску. Заводити облікові записи лише у системах, де вони потрібні.


Рис.1.6. Процес проведення атаки для отримання привілейованого доступу

3. *Видалити всі облікові записи та привілеї, які більше не потрібні*

При переводах та звільненні працівників часто виникають проблеми з безпекою, пов'язані з наявністю прав, яких не має бути у працівників. У випадку із зовнішніми підрядниками управління ситуацією ще складніше, особливо якщо доступ потрібен лише для короткострокового проекту.

*4. Формалізувати політику паролів*

Компанії з високим рівнем безпеки зазвичай застосовують формалізовану політику паролів для привілейованих облікових записів. Крім стандартних вимог, характерних для всіх облікових записів, слід заборонити або посилити контроль за спільним використанням привілейованих облікових записів.

*5. Впровадження технологій для контролю привілейованого доступу управління паролями*

Чим більше компанія, тим складніше буде управляти привілейованими доступом [4]. Багато хто починає з впровадження ПО, розробленого під задачу управління паролями привілейованих облікових записів. Ці рішення контролюють доступ до привілейованих облікових записів, генерують надійні паролі і зберігають їх в захищеному вигляді:

Надійні паролі ускладнюють задачу хакерів. Паролі управляються централізовано, так їх легше захистити.

Рішення PAM автоматизують процеси, що робить можливим створення і ротацію надійних паролів навіть для десятків тисяч облікових записів.

Рішення PAM дозволяють надавати привілейований доступ на обмежений час або протягом певних проміжків часу (наприклад для тимчасових проектів).

Однак системи управління паролями мають свої обмеження. Після компрометації облікових даних зловмисники можуть вільно переміщатися по мережі. Більш того, ці інструменти не надають інформацію про дії зловмисників після вторгнення. Щоб знизити ризик атак, пов'язаних з крадіжкою привілейованих облікових записів, організаціям необхідні додаткові методи захисту.

*6. Впровадити управління сесіями*

Скомпрометувавши привілейовані облікові записи, зловмисники можуть завдати величезної шкоди. Рішення для управління сесіями забезпечують централізований контроль доступу, надаючи ряд переваг:

– централізоване управління політиками, які дозволяють обмежити активність користувачів.

– моніторинг дій привілейованих користувачів в режимі реального часу.

– запис сесій надає можливість відслідковувати за діями тих, хто має доступ до важливих систем.

– подвійний контроль з авторизацією супервайзера для роботи в особливо критичних системах.

– оповіщення та розрив сесій в разі порушення політик.

Управління сесіями знижує ризик злому або несанкціонованого доступу до важливих активів IT системи організації, обмежуючи типи активів, до яких можна

отримати доступ, і типи команд, які можуть бути виконані. Однак, це не дозволяє оперативно виявляти факти компрометації облікових записів. У цьому допомагають технології машинного навчання і аналітики [4].

*6. Аналітика поведінки користувачів для контролю привілейованого доступу*

Цільові атаки часто використовують інструменти нульового дня для реалізації сценаріїв атак. Традиційні рішення по ІБ, такі як SIEM, часто не справляються із завданням виявлення, так як використовують методи детектування, засновані на правилах. Багато типів атак залишаються непоміченими. Саме цю проблему закриває аналітика поведінки користувачів. Характеристики набору тексту, дозвіл екрана нашого комп'ютера, смартфона або планшета, улюблені програми або веб-сайти та багато іншого є нашими цифровими слідами, які характеризують користувача не менше, ніж вички для зловмисників в IT-середовищі.

## 1.4. Аналіз технології управління привілейованого доступу користувачів інформаційної системи організації

У «Магічному квадранті Gartner 2024» для управління привілейованим доступом (PAM) було визначено деякі ключові тенденції, що підкреслюють критичну потребу в рішеннях PAM та стимулюють їхнє впровадження [7]:

1. Зростання кількості кібератак – зокрема, Gartner зазначив кілька гучних порушень, тісно пов’язаних зі зломом облікових даних привілейованих облікових записів та зловживанням привілеями протягом минулого року [7].

2. Вимоги до кіберстрахування – за даними Gartner, 15–25% їхніх клієнтів, які оцінюють інструменти PAM для першої покупки, заявляють, що роблять це, оскільки їхнє страхування кібербезпеки вимагає розгортання таких інструментів [7].

3. Віддалений доступ для постачальників та віддалених зовнішніх IT-персоналів – Gartner зазначив, що забезпечення привілейованого віддаленого доступу за допомогою інструментів PAM (а не лише інструментів віддаленого

доступу без привілейованого контролю) є рекомендованою найкращою практикою для виконання вимог та зменшення ризиків безпеки. Зростаюче визнання цієї найкращої практики організаціями призвело до збільшення продажів спеціалізованих інструментів RPAM (віддалене керування привілейованим доступом) [7].

Інші ринкові тенденції, які Gartner визначив як такі, що продовжують стимулювати впровадження PAM, включають [7]:

– динаміка ринку, що розвивається, для нових правил;
– прискорена міграція до хмари;
– впровадження автоматизації для DevOps;
– розмиття периметрів безпеки підприємства.


Рис.1.7. Магічний квадрант управління привілейованим доступом

Gartner визначає шість різних варіантів використання PAM:

1. Керування привілейованими обліковими записами та сеансами (PASM).

2. Керування підвищенням прав доступу та делегуванням прав Windows (PEDM).

3. PEDM для UNIX/Linux та macOS.

4. Управління секретами.

5. Керування правами доступу до хмарної інфраструктури (CIEM).

6. Віддалене керування привілейованим доступом (RPAM).

На рис. 1.8. показано рейтинг рішень PAM, які використовують максимальні кейси їх впровадження.

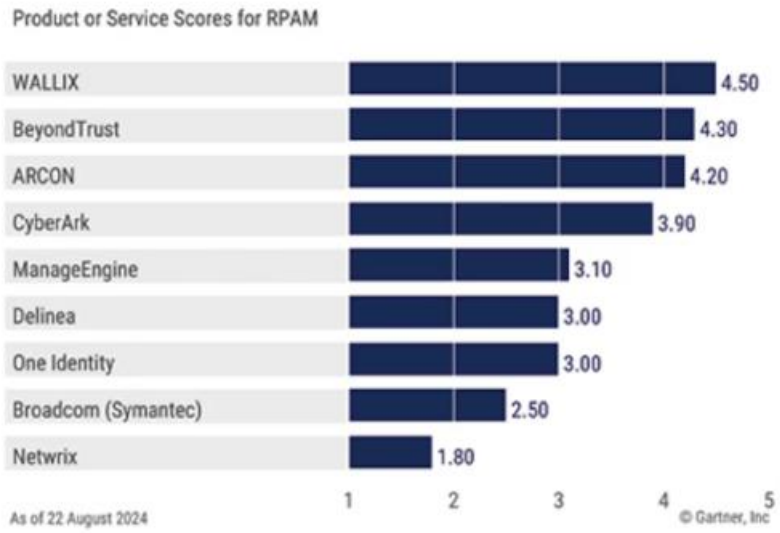


Рис.1.8. Рейтинг рішень PAM, які використовують максимальні кейси їх впровадження

Розглянемо рішення, які демонструють фундаментально архітектурні філософії, що безпосередньо впливають на їхню масштабованість, складність впровадження та загальну операційну стійкість. Розглянемо для порівняння три рішення.

*BeyondTrust*

BeyondTrust позиціонує себе як єдину, інтегровану платформу, розроблену для виявлення, контролю та захисту всіх шляхів до привілеїв (Paths to Privilege). Ця філософія є відповіддю на тенденцію до фрагментації інструментів безпеки.

Уніфікований підхід має на меті спростити розгортання, знизити витрати та підвищити легкість використання, забезпечуючи найглибший набір можливостей

управління привілейованим доступом та безпеки ідентичностей. Платформа BeyondTrust активно розширює покриття на критично важливі та нові сфери, включаючи безпеку хмарного доступу, захист операційних технологій, виявлення та реагування на загрози ідентичності (ITDR) та навіть оцінку ризиків, пов'язаних зі штучним інтелектом (AI Security). Забезпечення єдиної точки контролю для цих різнорідних систем є ключовою архітектурною перевагою, що робить платформу добре підготовленою для організацій, які переживають масштабну цифрову трансформацію або мають конвергентні IT/OT-середовища.

*One Identity Safeguard*

One Identity Safeguard вирізняється своєю архітектурою, орієнтованою на спеціалізовані аплайнси (програмно-апаратні комплекси, або їх віртуальні аналоги), які поділяються на дві ключові категорії: Safeguard for Privileged Passwords (SPP) та Safeguard for Privileged Sessions (SPS).

Safeguard for Privileged Passwords (SPP) фокусується на автоматизації та безпеці видачі привілейованих облікових даних.

Safeguard for Privileged Sessions (SPS) призначений для контролю, моніторингу та запису привілейованих сесій.

Ключовою особливістю Safeguard є його надійна кластерна архітектура, розроблена для високої доступності та аварійного відновлення. SPP дозволяє об'єднувати 3 або 5 аплайнсів у єдиний кластер. Усі важливі дані реплікуються всередині кластера, і система залишається повністю функціональною, навіть якщо деякі аплайнси виходять з ладу. SPS використовує дещо інший підхід для високої доступності / аварійного відновлення: він забезпечує відмовостійкість через незалежну конфігурацію "гарячого запасу" (hot-spare pair), тоді як масштабованість та спільне керування досягається кластеризацією кількох SPS-аплайнсів. Цей підхід ідеально підходить для високорегульованих галузей, де гарантована стійкість (99.999%) системи є більш критичною, ніж простота управління.

*ARCON*

ARCON PAM є комплексною модульною платформою з гнучкою архітектурою. Вона підтримує концепцію Віртуального Групування користувачів

та ресурсів, що надає гнучкість для управління кількома департаментами або філіями в межах однієї інфраструктури. Керування відбувається через єдину консоль адміністратора (One Admin Control).

Незважаючи на заявлену функціональність єдиної консолі, порівняльні оцінки користувачів вказують на потенційні операційні недоліки. Користувачі оцінили Централізоване Управління ARCON значно нижче порівняно з BeyondTrust . Це свідчить про те, що, хоча архітектура ARCON є гнучкою і конкурентною за ціною, реалізація централізованого управління у великих і складних середовищах може виявитися менш інтуїтивною або ефективною, що, як правило, збільшує операційні витрати (OpEx) на адміністрування та підтримку політик безпеки.

Аналіз ефективності кожного рішення вимагає порівняння їхніх реалізацій чотирьох ключових функціональних напрямків PAM.

A. Управління привілейованими обліковими даними та секретами

Усі три рішення надають основний функціонал сховища (Vaulting) та автоматизованої ротації паролів, що є невід'ємною вимогою PAM.

ARCON явно підкреслює свою здатність до Discovery (виявлення) та Onboarding (включення до системи) привілейованих ідентичностей з різноманітних джерел, включаючи хмарні платформи (AWS, Azure, GCP) та локальні каталоги (Microsoft AD), до єдиної консолі. Це має вирішальне значення для зменшення загрози, пов'язаної з покинутими або неконтрольованими привілейованими обліковими записами. BeyondTrust також фокусується на виявленні та правильному визначенні розміру (right-sizing) привілеїв , що відображає проактивний підхід до гігієни облікових записів. One Identity SPP призначений саме для надійного та автоматизованого зберігання і видачі облікових даних.

B. Управління привілеями кінцевих точок (EPM) та принцип найменших привілеїв (Least Privilege).

Ефективне управління привілеями на кінцевих точках є ключовим для мінімізації площі атаки та запобігання підвищенню привілеїв.

BeyondTrust демонструє лідерство у цьому напрямку. Його Endpoint Privilege Management для Windows Servers є однією з найсильніших пропозицій на ринку. Рішення дозволяє системним адміністраторам працювати як стандартні користувачі, підвищуючи привілеї лише для конкретних, авторизованих завдань через детальні, політико-орієнтовані елементи керування. Це забезпечує повний, гранульований контроль над операціями Windows, включаючи редагування реєстру, виконання скриптів, встановлення патчів та керування командним рядком (наприклад, PowerShell). Завдяки цій можливості організації можуть повністю усунути локальні права адміністратора, що, як підтверджують користувачі, призводить до зменшення ризиків та зниження кількості звернень до технічної підтримки. Функція Seamless Application Control забезпечує білий список додатків, використовуючи гнучкі політики та механізми Challenge/Response.

ARCON пропонує гранульований контроль доступу на основі принципів "need-to-know" та "need-to-do" , а також забезпеченням Least Privileges на кожну цифрову ідентичність. Хоча ці функції є заявленими, глибина та зрілість EPM-інструментарію BeyondTrust, підтверджена детальними описами можливостей, є помітною перевагою.

C. Керування сесіями, моніторинг та аудит

Здатність записувати та відтворювати привілейовані сесії є критичною для цифрової криміналістики (forensics) та виконання вимог комплаєнсу.

BeyondTrust виділяється завдяки високим оцінкам користувачів за функцію "Live session recording & playback". Така висока оцінка свідчить про якість, надійність та зручність інструментів для аудиту та моніторингу активності привілейованих користувачів, що є незамінним у контексті ITDR та швидкого реагування на інциденти. Платформа забезпечує повне ведення журналів та аудит усіх привілейованих дій.

ARCON включає Live Dashboard для перегляду активності в реальному часі та забезпечує повний аудит усіх виконаних команд. Однак, якщо порівнювати з конкурентом, користувачі не надали ARCON таких високих оцінок у цій сфері , що

може вказувати на меншу деталізацію записів або складніший процес пошуку та відтворення.

One Identity Safeguard покладається на спеціалізований компонент SPS для контролю та моніторингу сесій. Розділення функціоналу забезпечує високу надійність процесу запису та зберігання аудиторських слідів, що відповідає вимогам найсуворіших регуляторних стандартів.

D. Автентифікація та динамічний доступ (MFA/JIT)

Ключовим елементом сучасної стратегії безпеки є посилена автентифікація та динамічне управління привілеями.

MFA (багатофакторна автентифікація): Різниця у реалізації MFA між рішеннями є значною. Користувачі оцінили функціонал MFA BeyondTrust за високим показником, тоді як ARCON отримав нижчий. Це відображає, що BeyondTrust має більш зрілий механізм автентифікації, який забезпечує безфрикційну валідацію привілейованих користувачів, що є фундаментальним для надійного підходу Zero Trust.

Just-in-Time (JIT) Privileges: ARCON чітко позиціонує JIT як частину свого рішення, заявляючи про можливість усунення постійних привілеїв (standing privileges) для забезпечення безпеки Zero Trust, включаючи хмарну інфраструктуру та успадковані додатки. Хоча BeyondTrust та One Identity реалізують JIT-подібні механізми через їхні EPM та сесійні політики, One Identity явно робить акцент на цьому як на ключовій перевазі для адаптації до динамічних середовищ.

Узагальнимо стратегічні переваги та потенційні ризики, пов'язані з кожним рішенням.

Таблиця 1.1.

Аналіз переваг та недоліків рішень

| **Рішення** | **Ключові Переваги (Advantages)** | **Ключові Недоліки (Disadvantages)** |
|---|---|---|
| **ARCON** | Конкурентоспроможне ціноутворення. Гнучке віртуальне групування ресурсів. Активний розвиток JIT та хмарних інтеграцій. Відкрита підтримка онбордингу з AWS, Azure, GCP. | Значний дефіцит у якості підтримки та централізованого управління. Слабша реалізація MFA порівняно з конкурентом. Складність адміністрування. |
| **BeyondTrust** | Найкраща у своєму класі EPM/Least Privilege. Виняткова якість аудиту та моніторингу сесій. Уніфікована платформа, готова до ITDR, OT та AI, що забезпечує майбутню стійкість. Високий рейтинг MFA та централізованого управління (9.4). | Висока вартість володіння (преміум-сегмент). Складність орієнтації у продуктовій лінійці через велику кількість спеціалізованих інструментів. |
| **One Identity Safeguard** | Спеціалізована кластерна архітектура для максимальної високої доступності та аварійного відновлення (SPP/SPS). Розділення функцій (Passwords/Sessions) для підвищеної стійкості. Відносно легка у навчанні. | Невисока вартість. Вимагає більших інвестицій у спеціалізовані ресурси) та їхнє обслуговування. |

One Identity Safeguard, з його аплайнс-орієнтованою, кластерною архітектурою (SPP/SPS), є ідеальним вибором для фінансового сектору, телекому та критичної інфраструктури, де забезпечення неперервності та надійної реплікації даних є абсолютним пріоритетом. Розділення функцій на спеціалізовані аплайнси підвищує архітектурну стійкість. Тож надалі продовжимо дослідження технології One Identity Safeguard.

# 2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ДАНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

## 2.1. Архітектура та модулі One Identity Safeguard

One Identity Safeguard для Privileged Passwords створено спеціально для використання рішення привілейованого управління Safeguard for Privileged Passwords, яке попередньо встановлено і готове до негайного використання. Рішення призначено, щоб гарантувати безпеку системи на рівні обладнання, операційної системи і програмного забезпечення. Посилене рішення захищає програмне забезпечення для привілейованого управління від атак, спрощуючи розгортання і поточне управління, а також скорочуючи терміни окупності.

*Пакет програмного забезпечення для привілейованого управління Safeguard*

Програмне забезпечення для привілейованого управління Safeguard використовується для контролю, моніторингу та управління обліковими записами і діями привілейованих користувачів з метою виявлення можливих зловмисних дій, виявлення ризиків, пов'язаних з наданням прав, і надання доказів несанкціонованого доступу. Safeguard також допомагає у розслідуванні інцидентів, проведенні цифрової криміналістики та дотриманні нормативних вимог.

До основних переваг продуктів Safeguard відноситься:

– Універсальне рішення для забезпечення управління привілейованим доступом;

– Легкість розгортання та інтеграції;

– Функція запису всіх сесій;

– Комплексний аналіз ризиків;

– Управління привілейованим обліковим записом.

У комплект входять наступні модулі:

*Safeguard for Privileged Password* автоматизує, контролює та захищає процес, що забезпечує доступність привілейованих облікових записів за допомогою управління доступом на основі ролей та автоматизованих робочих процесів.

Safeguard for Privileged Passwords захищає пристрої, усуває небезпеку за допомогою безпечного доступу до єдиного рішення. Це допомагає прискорити інтеграцію з інформаційною системою організації та IT-стратегіями. Крім того, інтерфейс користувача надає можливість управляти паролями з будь -якого місця та за допомогою будь-якого пристрою.

*One Identity for Privileged Sessions* є частиною рішення управління привілейованим доступом One Identity. Safeguard for Privileged Sessions представляє собою рішення щодо управління привілейованими сеансами, які забезпечують гарні показники в галузі контролю доступу, а також моніторингу та запису сеансів щодо запобігання неправомірному використанню привілейованих облікових записів, забезпечення відповідності.

*Privileged Sessions* - швидко розгортає корпоративне рішення, повністю незалежне від клієнтів та серверів та легко інтегрується в існуючі мережі. Він збирає дані про активність, необхідні для профілювання користувачів та забезпечує можливість повного аналізу сеансу користувача для проведення розслідувань.

*One Identity Safeguard for Privileged Analytics* об'єднує дані із Safeguard для Privileged Sessions, щоб використовувати їх у якості основи для аналізу подій, привілейованих користувачів. Захист для привілейованої аналітики використовує алгоритми машинного навчання для вивчення конкретних характеристик та створює профілі для кожного окремого привілейованого користувача. Захист для привілейованої аналітики порівнює фактичну активність користувачів із профілями користувачів у режимі реального часу, а профілі постійно коректуються за допомогою машинного навчання. Захист для привілейованої аналітики виявляє аномалії та ранжирує їх за ступенями ризику, це дозволяє розкладати пріоритети та розпочати відповідні дії та, у зв’язку з цим, запобігти витоку даних.

Як було відзначено раніше, рішення привілейованого доступ сфокусовано на трьох модулях [6]:

Safeguard for Privileged Passwords (SPP) - управління паролями;

Safeguard for Privileged Sessions (SPS) - управління сесіями;

Safeguard for Privileged Analytics (SPA) - аналіз поведінки.

Архітектура взаємозв'язку модулів представлено на рис.2.1.

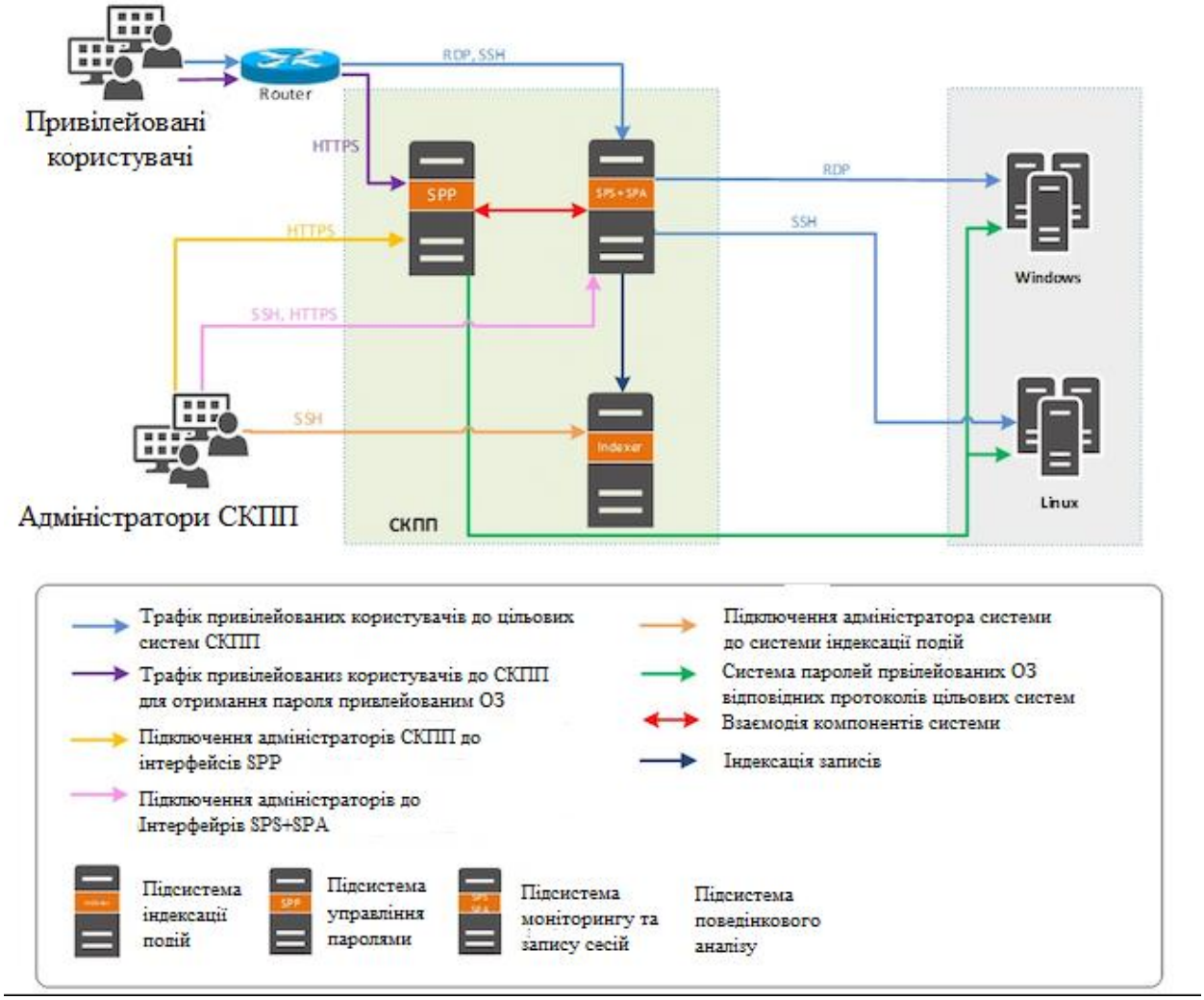


Рис.2.1. Архітектура захисту привілейованих користувачів

Кожен з модулів рішення представлено у вигляді одного з блоків. Отже, рішення дозволяє створювати відмовостійкі конфігурації. Особливістю рішення є те, що One Identity Safeguard працює на мережевому рівні без необхідності установки агентів на кінцеві машини. Дана особливість підвищує легкість використання рішення, як адміністраторам так підрядникам. Тому не потрібно переводити їх на використання незручних інструментів, що також прискорить час впровадження рішення, як для проведення тестових випробувань, так і в режимі робочої експлуатації для постійного функціонування.

Архітектура рішення Safeguard привілейованого доступу показано на рисунку 2.2.

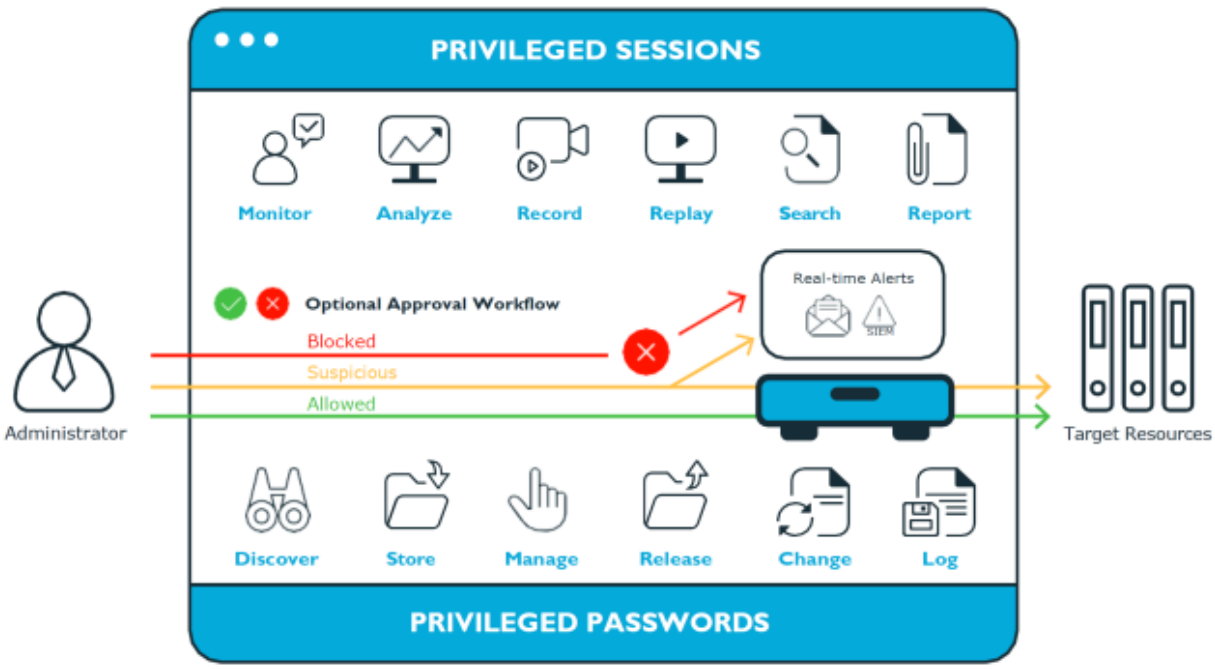


Рис.2.2. Архітектура привілейованого доступу Safeguard

Тож надалі розглянемо функції кожного з модулів рішення.

## 2.2. Функції модуля Safeguard for Privileged Passwords

Privileged Passwords

Privileged Passwords входять наступні логічні об’єкти: сховище паролів, ключів і секретів для захисту активів, включаючи комп'ютери, сервери, мережеві пристрої, каталоги та програми (рис. 2.3).

Визначимо засоби захисту привілейованих паролів, такі як активи, розділи та профілі та їх взаємозв’язок.

До логічних об’єктів належать комп’ютери, сервери, мережеві пристрої, каталоги або програми, якими може керувати Safeguard. Об’єкти мають пов’язані облікові записи користувачів та облікові записи служб. Активи та рахунки можуть

бути імпортовані (наприклад, з Active Directory). Активи можуть бути або не бути частиною групи активів.

Модуль Privileged Passwords використовує *розділи* з контейнером для делегованого управління паролями облікових записів і ключами SSH (включаючи перевірку та зміну). Розділи необхідні для розподілу активів між різними власниками для розподілу обов'язків (SoD - Separation of Duties). Розділи дозволяють налаштувати кілька менеджерів активів, кожен з яких має можливість визначати правила паролів для керованих систем у їх власній робочій області. Зазвичай активи необхідно розділити за географічним розташуванням, власником, функцією або операційною системою. Наприклад, можна згрупувати ресурси Unix у розділі та делегувати їх адміністратору Unix для управління ним. Кожен модуль повинен мати власника розділу. Актив може бути призначений лише до одного розділу одночасно. Коли призначається об'єкт до розділу, усі облікові записи, пов'язані з цим об'єктом, також автоматично перепризначуються до цього розділу. Потім усі нові облікові записи, які додаються для цього активу, автоматично призначаються цьому розділу.

*Профіль Privileged Passwords* включає в себе розклади та правила, що регулюють призначені активи розділу та рахунки активів. Наприклад, профіль визначає, як часто необхідна перевірка пароля для активу або облікового запису.

*Розділ* може мати кілька *профілів,* кожен з яких, за бажанням, призначається різним ресурсам. Обліковим записом керує лише один профіль. Якщо обліковий запис явно не призначений для профілю, обліковий запис керується тим, який призначений материнському активу. Якщо цей об'єкт не має призначеного профілю, призначається профіль розділу за замовчуванням.

При створенні нового розділу, Safeguard for Privileged Passwords створює відповідний профіль за замовчуванням із розкладами та правилами за замовчуванням. Тож можна створити декілька профілів для керування обліковими записами, призначеними для розділу. *Активи та рахунки* відносяться до сфери дії профілю.

Наприклад, припустимо, що є актив із 12 обліковими записами, і ми налаштували профіль на перевірку та зміну паролів кожні 60 днів. Якщо ми хочемо, щоб пароль керувався одним з цих облікових записів кожні сім днів, ми можемо створити інший профіль і додати обліковий запис до нового профілю. Тепер Safeguard for Privileged Passwords перевірятиме та змінюватиме усі паролі до цього активу кожні 60 днів, за винятком цього облікового запису, який буде змінюватися кожні сім днів.

У наведеному нижче прикладі розділ А має три профілі (профіль А, В та С) та стандартний профіль. Профіль А перевіряє паролі кожні 30 днів. Профіль В перевіряє паролі кожні три місяців, а профіль С має найвищий рівень безпеки, перевіряючи паролі кожні сім днів (рис.2.3). Рисунок 2.3 ілюструє як сервер ресурсів має два профілі, кожен з яких керує різними обліковими записами пов'язані з активом. Профілі А, В і С явно призначаються обліковим записам та показаним активам. Хмарний сервіс не має активів чітко призначених профілю, тому файл за замовчуванням буде використовуватися для управління обліковими записами активу.

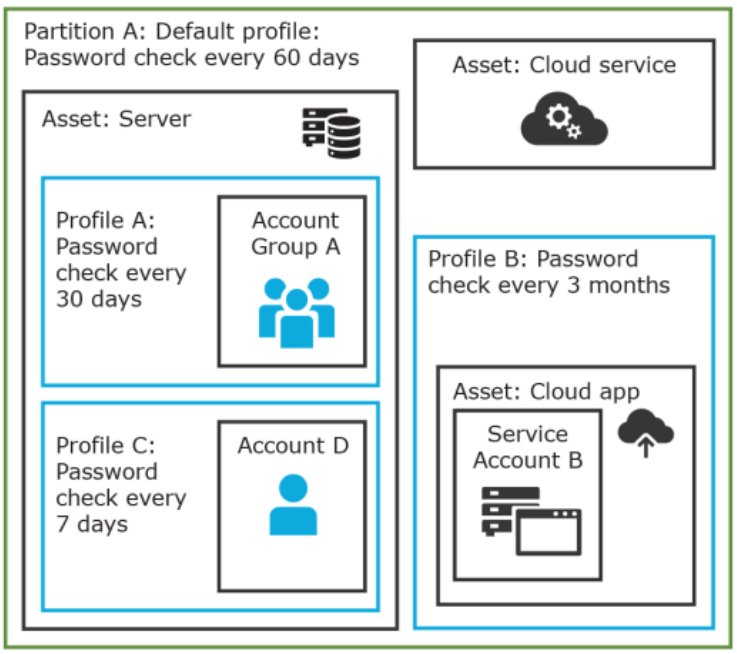


Рис. 2.3. Контроль паролів: розділ, профіль актив

Розглянемо що представляють собою активи і групи активів.

Активом може бути комп’ютер, сервер, мережевий пристрій, каталог або програма.

До об’єкта увійти можна за кількома обліковими записами, але обліковий запис має бути пов’язаний лише з одним об’єктом.

Якщо обрати об’єкт для профілю, усі облікові записи будуть включені.

Актив має бути призначений лише одному розділу. Об’єкт зазвичай має профіль, але він не є обов’язковим.

Є можливість створити кілька об’єктів для одного пристрою чи програми, а потім керувати різними обліковими записами для кожного об’єкта.

Група активів - це набір активів, які можна додати до сфери політики запитів на доступ до прав.

Визначимо що представляють собою розділи та профілі.

Розділ - це група активів (і пов’язаних облікових записів активів), що керуються профілем і використовуються для делегування управління активами. Актив може бути одночасно лише в одному розділі. Усі облікові записи, пов’язані з цим об’єктом, автоматично додаються до розділу.

Профілі - це розклади та правила, які регулюють активи розділу та рахунки активів. Можна встановити профіль за замовчуванням для призначення або можна вручну призначити профіль активу або обліковому запису.

Коли створюється розділ, для нього створюється профіль за замовченням. Цей профіль неявно асоціюється з усіма активами та обліковими записами, доданими до розділу. Пізніше до активів та облікового запису можна вручну призначити інший профіль, який називається явною асоціацією. Явні асоціації (призначення вручну) замінюють неявні асоціації (автоматичні призначення).

### 2.3. Функції модуля Privileged Sessions

One Identity Safeguard for Privileged Sessions (SPS) є частиною рішення One Identity Safeguard, яке є частиною рішення управління привілейованим доступом One Identity. Для задоволення потреб великих підприємств SPS – це привілейоване

рішення для управління сеансами, яке забезпечує кращий контроль доступу, запис сеансів та аудит для запобігання зловживань привілейованими обліковими записами та кращого розслідування.

SPS — це інструмент для організацій, який швидко розгортається, повністю є незалежним від клієнтів і серверів, та легко інтегрується в існуючі мережі організації. Дане рішення фіксує дані про діяльність, необхідні для профілювання користувачів, і дає змогу детально аналізувати сеанс користувача для проведення розслідувань.

SPS має повний контроль над з'єднаннями SSH, RDP, Telnet, TN3270, TN5250, Citrix ICA і VNC, створюючи структуру (з чіткими межами) для роботи адміністраторів.

Основні характеристики SPS:

*Централізоване застосування політик*.

SPS діє як централізована точка автентифікації та контролю доступу в IT-середовищі, яке захищає від привілейованих крадіжок особистих даних та зловмисників. Детальне управління доступом допомагає контролювати, хто і коли може отримати доступ до ваших критичних IT -ресурсів.

*Запобігання зловмисним діям*

SPS відстежує сеанси привілейованих користувачів в режимі реального часу і виявляє порушення політик в міру їх виникнення. У разі виявлення підозрілої активності користувача (наприклад, введення не дозволеної команди, такої як «rm»), SPS може надіслати попередження або відразу розірвати з'єднання.

*Велика відповідальність (стримування)*

SPS перевіряє, «хто що робив», наприклад, у базі даних або серверах SAP. Знаючи це, співробітники будуть виконувати свою роботу більш відповідально, що призводить до скорочення людських помилок. Маючи легку інтерпретацію і захищений від несанкціонованого доступу запис в зашифрованому журналі аудиту з мітками часу і цифровим підписом, відбитком пальця можуть бути усунені.

*Швидкі та економічні перевірки відповідності*

SPS дозволяє відстежувати всі дії користувачів, записуючи їх у високоякісних, захищених від несанкціонованого доступу журналах аудиту. Всі дані зберігаються в зашифрованих файлах з відмітками часу і підписом, що запобігає будь-які зміни або маніпуляції. Журнали аудиту, схожі на фільми та гарантують, що вся необхідна інформація буде доступна для спеціального аналізу або аудиторських звітів.

*Зниження витрат на пошук і усунення несправностей і проведення розслідувань*

Коли щось відбувається не так, необхідно дізнатись справжню історію. Аналіз тисячі текстових журналів може бути нескінченим і може застосовувати участь зовнішніх експертів. Можливість легко відновити сеанси користувачів дозволяє скоротити час дослідження і уникнути непередбачених витрат.

*Особливості застосування та роботи SPS*

One Identity Safeguard для привілейованих сеансів (SPS) - це мережевий пристрій під ключ - його реалізація і настройка виконуються швидко і просто. У порівнянні з конкурентами, немає необхідності купувати і встановлювати будь-яке додаткове програмне забезпечення (наприклад, сервери Windows або MS SQL) або обладнання для повноцінної роботи SPS.

Для реалізації рішення достатньо декілька днів днів.

Впровадження та налаштування може відбуватися без залучення дорогих професійних послуг. Після розгортання SPS працює у фоновому режимі, як чорний ящик літака - для його роботи немає необхідності в додатковому робочому навантаженні.

*SPS -незалежний пристрій без агентів.*

У порівнянні з рішеннями на основі агентів немає необхідності в установці і оновленні агентів на клієнтах або серверах, що виключає непотрібне обслуговування і потенційні проблеми з безпекою. В якості шлюзу, незалежного від хоста, SPS може контролювати і відслідковувати доступ до будь-яких типів систем, таких як сервери Windows / UNIX / Linux, мережеві пристрої, пристрої безпеки, веб-додатки або середовища тонких клієнтів.

*SPS прозорий, «роутерний» режим роботи.*

В якості проксі-шлюзу SPS може працювати як маршрутизатор в мережі, невидимо для користувача і сервера. В якості прозорого рішення SPS вимагає мінімальних змін існуючої мережі. Крім того, оскільки він працює на мережевому рівні, користувачі можуть продовжувати використовувати клієнтські програми, з якими вони знайомі, і їм не потрібно змінювати свої робочі процеси.

*Детальний контроль доступу*

Оскільки SPS має повний доступ до трафіку який перевіряється, фахівці безпеки можуть детально контролювати, хто і коли отримав доступ до серверів. Наприклад, можна вибірково дозволити або заборонити доступ до каналів протоколу: дозволяти термінальні сеанси в SSH, але відключати переадресацію портів і передачу файлів, або дозволяти доступ до робочого столу для RDP, але відключати спільне використання файлів. Крім того, SPS підтримує тіньове копіювання в реальному часі, дозволяючи стежити за сеансом адміністратора в режимі реального часу і розривати його / її з'єднання в разі виявлення порушення політики.

*Запобігання шкідливих дій в режимі реального часу*

SPS може відстежує переданий контент в режимі реального часу і відправляє попередження або навіть блокує з'єднання, якщо в трафіку виявиться певний шаблон. Визначені шаблони можуть бути небезпечною командою в текстовому протоколі або підозрілими додатками в графічному з'єднанні. Ці політики на рівні команд і додатків можуть запобігати зловмисним діям користувачів у міру їх виникнення, а не просто записувати їх або повідомляти про них.

*Запис і аудит сесій*

SPS - це рішення для аудиту сеансів, що пропонує можливості оптичного розпізнавання символів для реєстрації всіх даних про привілейовані дії в графічних додатках для інтерфейсів користувача, а також в текстових протоколів. SPS також може підтримувати і перевіряти передачу файлів. Всі дані записуються в журнали аудиту, як фільми, з можливістю пошуку, що спрощує пошук необхідної інформації в розслідуваннях інцидентів. У разі виникнення проблем (неправильна

конфігурація сервера, маніпуляції з базою даних, несподіване завершення роботи) причини події легко доступні в журналах аудиту, тому причини інциденту можна легко визначити.

Щоб захистити конфіденційну інформацію, включену в обмін даними, два напрямки трафіку (клієнт-сервер і сервер-клієнт) можуть бути розділені і зашифровані за допомогою різних ключів, тому конфіденційна інформація, така як паролі, відображається тільки при необхідності.

SPS підтримує прозорі і непрозорі режими роботи проксі, щоб максимально спростити розгортання в існуючих мережевих інфраструктурах. SPS буде автоматично обробляти непрозорі і прозорі з'єднання одночасно.

Є декілька режимів роботи SPS:

*Непрозорий проксі,* який найпростіше реалізується. У такій конфігурації клієнти підключаються до сервера через SPS. Тобто кінцеві користувачі явно звертаються до SPS, який потім перенаправляє підключення до цільових систем на основі різних параметрів.

*Прозорий режим*, якщо налаштовується проксі SPS в прозорому режимі, клієнт зазвичай звертається до цільового сервера безпосередньо. Отже, необхідно відповідним чином налаштувати політики підключення в SPS.

*Прозорий режим з одним інтерфейсом.* У цьому режимі основна увага приділяється роботі непрозорого проксі, яку найпростіше реалізувати. У цій конфігурації клієнти підключаються до сервера через SPS. Тобто кінцеві користувачі явно звертаються до SPS, який потім перенаправляє підключення до цільових систем на основі різних параметрів залежно від того, який метод вибору місця призначення ви вибрали.

### 2.4. Функції модуля  Privileged Privileged Analytics

One Identity Safeguard для привілейованих сеансів об'єднує дані з SPS, щоб використовувати їх в якості основи для аналізу поведінки користувачів. SPA використовує алгоритми машинного навчання для вивчення поведінкових

характеристик і генерує профілі поведінки для кожного окремого привілейованого користувача. SPA порівнює фактичну активність користувачів з профілями користувачів в режимі реального часу, причому профілі постійно коригуються за допомогою машинного навчання. Коли SPA виявляє незвичну активність, це відображається в інтерфейсі SPS у вигляді високих балів і інформацією на дашборді [7].

Отже, що SPA працює в поєднанні з SPS. До основних вимог для нормальної роботи SPA відноситься:

1. Для нормальної роботи SPA потрібно не менше 12 ГБ ОЗУ.

2. SPA вимагає великої кількості обчислень, що може чинити вплив на SPS:

2.1. Алгоритм натискання клавіш набагато більш вимогливий до ресурсів, ніж інші алгоритми, тому рекомендується почати аналіз даних з використанням алгоритмів, що вимагають менше ресурсів.

2.2. Перш ніж почати використовувати SPA, переконатися, що доступна принаймні половина зазначеною ємності SPS.

3. SPA аналізує тільки контрольні журнали і метадані SPS, але не аналізує дані журналів.

Для того щоб проводити аналітику при роботі з привілейованими користувачами та виявляти порушення в системі управління привілейованими користувачами використовуються спеціальні алгоритми, які використовує One Identity Safeguard для Privileged Analytics.

One Identity Safeguard для Privileged Analytics аналізує поведінку користувачів за допомогою алгоритмів, також званих аналітикою.

Алгоритми One Identity Safeguard для Privileged Analytics є математичні методи, які можна використовувати для аналізу даних сеансу з різних сторін. Алгоритми необхідно навчати з використанням історії даних сеансу. На основі цього навчання алгоритм може побудувати базову лінію поведінки конкретного користувача і оцінити нові сеанси. Бали такої оцінки покажуть, чи є поведінка конкретного користувача нормальною або аномальною в порівнянні з базовим

рівнем. Алгоритми також забезпечують візуалізацію для відображення інформації про поведінку користувача [10].

Основні алгоритми Privileged Analytics для аналізу:

*Алгоритм натискання клавіш* може вказати, чи дії користувача є дійсними, чи це той користувач. Даний алгоритм заснований на динаміці помилок адміністраторів. SPA компілює профіль набору тексту для кожного користувача в залежності від того, скільки секунд зазвичай потрібно користувачеві, щоб натискати комбінації клавіш на своїй клавіатурі. Алгоритм натискання клавіш аналізує дані клавіатури, що надходять з сеансів RDP або SSH, і порівнює їх з профілем користувача.

*Алгоритм команди*. SPA компілює профіль команд для користувача на основі команд, які вони зазвичай виконують. Алгоритм команди визначає ймовірність настання певних команд протягом сеансу.

*Алгоритм часу входу* будує профіль, заснований на точному часу кожен день, тобто враховує коли користувач входить в систему. На основі профілю користувача, він може виявити, який час для даного логіна є незвичайним або аномальним, враховуючи щоденний розподіл входу користувача подій для попереднього часу.

*Алгоритм логіна* для аналізу, схожості двох хостів заснованих на користувачі, для входу на ці хости. Коли користувач входить в систему на хості, на який він ніколи або дуже рідко входить в систему, це не буде вважатися аномалією, якщо цей хост схожий на інші хости, які користувач часто використовує.

*Алгоритм частого набору товарів* схожий на «Алгоритм частого набору товарів» (fis), який схожий на алгоритм типу «Клієнти, які купили ці товари, також купили», який використовується на веб-сайтах електронної комерції. Він досліджує кілька атрибутів сеансів і намагається знайти значення, які часто зустрічаються разом, утворюючи набір. Використовуючи цю інформацію, алгоритм fis може виявляти закономірності в поведінці користувачів, наприклад, «ця людина використовує RDP тільки посеред ночі з цього IP-адреси».

*Алгоритм заголовка вікна* аналізує заголовки вікон, щоб розкрити незвичайну поведінку користувача, тобто, він ідентифікує користувачів на основі того, яке має назву вікно, яке вони зазвичай мають на своєму екрані. В даний час це експериментальний алгоритм, який за замовчуванням відключений.

*Алгоритм аутентифікації миші* користувача – алгоритм на основі руху миші може повідомити, чи є користувач тим, кого представляє, на підставі рухів їх миші.

*Виявлення сеансу за сценарієм* визначає, вказують чи дійсно дії в сеансі відповідають заданому сеансу за сценарієм. Наступні внутрішні алгоритми в фоновому режимі допомагають визначити, чи є сеанс сценарієм.

*Алгоритм clockmaster* здатний виявити неприродні точні сеанси, які починаються неодноразово в певних пікових хвилинах години (наприклад, о 8:30, 10.30, 11:30, і так далі). Алгоритм позначає такі сеанси як сеанси за сценарієм. Причина цього в тому, що хвилини в мітках часу людської діяльності за більш тривалий період часу імовірно мають випадковий рівномірний розподіл або дуже близькі до нього.

*Алгоритм Gapminder* здатний виявляти скріптові сесії на основі часових проміжків між сесіями, які належать до даного рахунку. Коли проміжки часу між сеансами мають типові повторювані значення, це говорить про аномальну періодичну поведінку. Алгоритм розриву не будує базові показники. Замість цього він постійно перевіряє проміжки часу однакової тривалості між сеансами. Якщо є чотири послідовні сеансу з однаковими часовими інтервалами між ними, і за ними слідує п'ята сесія з таким же тимчасовим інтервалом, то алгоритм позначає п'ятий сеанс як сеанс за сценарієм.

SPA автоматично запускає інструмент оцінки алгоритмів кожен день, щоб оцінити, наскільки добре ці алгоритми аналітики працюють з поточним набором даних, що знаходяться в розгортанні SPS.

Визначивши функції основних модулів рішення One Identity Safeguard, щодо захисту привілейованого захисту користувачів інформаційної системи організації, розробимо варіант налаштування та реалізації даної технології.

# 3 РОЗРОБЛЕННЯ ВАРІАНТУ ТЕХНОЛОГІЇ УПРАВЛІННЯ КОРИСТУВАЧАМИ ПРИВІЛЕЙОВАНОГО ДОСТУПУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ ONE IDENTITY SAFEGUARD

## 3.1. Технологія налаштування Safeguard for Privileged Passwords

Розглянемо робочий процес запиту доступу Safeguard for Privileged Passwords.

Система One Identity Safeguard for Privileged Passwords (SPP) функціонує як централізований шлюз для контрольованого надання привілейованого доступу. На операційному рівні, кінцевий користувач або інтегрований додаток ініціює запит на отримання критичних облікових даних (пароля або ключа SSH) або на встановлення проксі-сеансу (наприклад, RDP, SSH, Telnet) до цільового активу [7]..

Ключовим моментом є механізм контролю робочого процесу: ініційований запит може бути автоматично схвалений або ж вимагати попереднього затвердження відповідно до встановлених політик. Після успішного підтвердження, запитувані облікові дані стають доступними для використання або ж відкривається захищений сеанс. Усі проксі-сеанси обов'язково проходять через компонент Safeguard for Privileged Sessions і повністю записуються [7].

По завершенні роботи з привілейованими даними або сеансом, система дозволяє провести процедуру перевірки, що підтверджує завершення активності користувача. Політика доступу може вимагати цю перевірку перед наступним доступом. Для запитів, пов'язаних з паролями, політика також може бути налаштована на автоматичну зміну облікових даних після їх використання, що значно підвищує безпеку.

Для привілейованих паролів доступні наступні функції представлені в таблиці 3.1.

Таблиця 3.1.

Можливості One Identity Safeguard for Privileged Passwords

| Характеристика | Опис |
|---|---|
| Автоматична авторизація | Автоматичний вхід в систему і запуск запиту доступу до сеансу підвищує безпеку і відповідність вимогам, оскільки облікові дані облікового запису ніколи не розкриваються користувачеві. |
| Activity Center | Використовуючи Activity Center, можна швидко і легко переглянути всі дії, які виконуються користувачами Safeguard for Privileged Passwords, і інтегровані процеси. У звітах Activity Center можна виконувати пошук, налаштовувати і фільтрувати дані, щоб зосередити увагу на діях одного користувача або для аудиту багатьох дій в підмножині відділів. Крім того, можна запланувати запити, а також зберегти або експортувати дані. |
| Завжди онлайн | Захист привілейованих паролів. Пристрої можуть бути об'єднані в кластер для забезпечення високої доступності. Паролі, ключі SSH і сеанси можна запросити з будь-якого пристрою в кластері Safeguard for Privileged Passwords. |
| Підтвердження з будь-якого місця | Використовуючи One Identity Starling, можна схвалити або відхилити будь-який запит доступу в будь-якому місці, не перебуваючи в VPN. |
| Хмарна підтримка | Safeguard для привілейованих паролів можна запустити в хмарі за допомогою Azure або AWS. |

Для забезпечення відмовостійкості модуля SPP є можливість виконати кластеризацію рішення за технологією «active-active» [6].

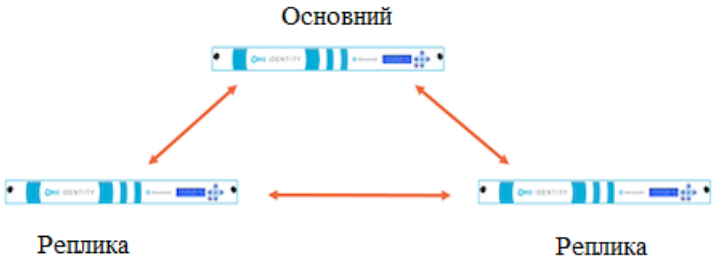


Рисунок 3.1. Архітектура кластера SPP

Мінімальна кількість машин для створення кластера - 3, так як для ухвалення рішення в кластері використовується поняття кворуму. Для розуміння цього процесу, уявимо собі сценарій, в якому зібраний кластер з трьох пристроїв (рис 3.1). Якщо через нештатну ситуацію одна з машин припинила роботу, то в кластері зберігається кворум, виконуються звичайні операції з надання та зміни паролів. Якщо «падає» другий пристрій, то в цей момент кворум втрачається і паролі на цільових системах перестають змінюватися (але продовжують надаватися). Після відновлення хоча б одного пристрою знову з'являється кворум і триває нормальна робота системи.

Для створення привілейованих користувачів можливо використовувати інфраструктуру каталогів (наприклад, Microsoft Active Directory). Для цього необхідно імпортувати користувачів каталогу та групи каталогу. Користувачі каталогу проходять автентифікацію в Safeguard for Privileged Passwords, використовуючи облікові дані каталогу. Користувачі керованих облікових записів не можуть бути членами групи безпеки AD «Захищені користувачі».

Дані Active Directory та LDAP автоматично синхронізуються схемою постачальників ресурсів або ключів та автентифікації, як показано в наведених нижче списках [7].

Для цього необхідно скласти список схем активів та список схем постачальників ідентифікації та аутентифікації.

**Список схем активів**

***Користувачі:***

Ім'я користувача

Пароль (змінюється на LDAP і не змінюється на Active Directory)

Опис

***Групи:***

Ім'я

Член

***Комп'ютер:***

Ім'я

Мережева адреса

Операційна система

Версія операційної системи

Опис

***Список схем постачальників ідентифікації та аутентифікації:***

Користувачі

Ім'я користувача

Ім'я

Прізвище

Робочий телефон

Мобільний телефон

Ел. адреса

Опис

Перевірка автентичності зовнішньої федерації

Радіус аутентифікації

Керовані об'єкти

***Групи:***

Ім'я

Члени

Опис

Створення таких каталогів надасть можливисті покращеної роботи з привілейованими записами

*Відкриття.* Швидко виявляє будь-який привілейований обліковий запис або систему у вашій мережі за допомогою параметрів виявлення хоста, каталогу та мережі.

*Параметри сповіщення про подію.* Safeguard for Privileged Passwords дозволяє настроїти пристрій для надсилання повідомлень про події у зовнішні системи, такі як електронна пошта, системний журнал та SNMP.

*Налаштування обраних параметрів* Швидкий доступ до паролів, які найчастіше використовуються, з головного екрана. Ви можете згрупувати кілька запитів пароля в одне обране, щоб отримати доступ до всіх потрібних облікових записів одним клацанням миші.

*One Identity Starling.* Розширення можливості Safeguard за допомогою One Identity Starling, яке пропонує швидкий доступ до хмарних функцій і послуг. Сюди входить універсальна двофакторна аутентифікація Starling (2FA) для захисту доступу Safeguard [8].

*Перегородки і профілі.* Функція Safeguard for Privileged Passwords дозволяє групувати керовані системи в безпечних робочих областях, які можна назначити для делегованого управління.

*Вільний контроль.* Управляє запитами паролів і ключів SSH від авторизованих користувачів для вхідних записів, за якими вони мають право доступу через безпечне з’єднання через веб-браузер із підтримкою мобільних пристроїв.

*RESTful API.* Safeguard for Privileged Passwords (SPP) побудований за принципом «спочатку API» і використовує модернізований API, заснований на архітектурі REST, який підтримує інші програми та системи. Кожна функція надається через API, щоб забезпечити швидку та легку інтеграцію, незалежно від того, що ви хочете робити або якою мовою написані ваші програми. Є навіть кілька речей, які можуть бути виконані лише через Safeguard SPP API.

*Керування доступом на основі ролей (RBAC).* Safeguard for Privileged Passwords використовує ієрархію керування доступом на основі ролей з використанням наборів дозволів адміністратора. Доступно безліч ролей для

адміністрування Safeguard для привілейованих паролів, що забезпечують детальне делегування та робочі процеси, а також найменш привілейований доступ.

*Безпечний доступ до застарілих систем.* Використовуйте смарт-картку, двофакторну автентифікацію або інші методи суворої автентифікації для отримання доступу до систем. Оскільки Safeguard для привілейованих паролів діє як шлюз або проксі-сервер для системи, він забезпечує надійну автентифікацію для цілей, які спочатку не можуть або не підтримують ці методи.

*Підтримка смарт-карток.* Аутентифікація привілейованих користувачів може бути інтегрована з підтримкою Microsoft Active Directory для смарт-карток або вручну завантажена в сам пристрій Safeguard for Privileged Passwords.

*Підтримка двофакторної автентифікаціїю.* Недостатньо захистити доступ до паролів іншим паролем. Підвищена безпека за рахунок вимоги двофакторної автентифікації для захисту привілейованих паролів. Safeguard for Privileged Passwords підтримує будь-яке рішення 2FA на основі Radius та служби двофакторної аутентифікації (2FA) компанії One Identity.

*Механізм робочого процесу для керування випуском на основі політик*. Використовуючи безпечний веб-браузер з підтримкою мобільних пристроїв, можна запитувати доступ та підтверджувати привілейовані паролі та сеанси. Запити можуть затверджуватись автоматично або вимагати подвійного/множинного затвердження залежно від політики організації. Механізм робочого процесу підтримує тимчасові обмеження, наявність кількох стверджуючих та перевіряючих, екстрений доступ та закінчення терміну дії політики.

Визначивши ключові функції Safeguard for Privileged Passwords визначимо основні кроки для налаштування Safeguard для привілейованих паролів вперше

Перш ніж One Identity Safeguard для привілейованих паролів зможе керувати паролями привілейованих облікових записів та привілейованими сеансами, необхідно спочатку додати всі об'єкти, необхідні для написання політик запитів доступу, такі як користувачі, облікові записи та активи. Дотримуючись цих процедур, створити ієрархію адміністраторів, яка забезпечить дотримання вашою компанією контролю доступу на основі ролей.

Перш ніж Safeguard for Privileged Passwords зможе скидати паролі локальних облікових записів у системах Windows, необхідно змінити локальну політику безпеки, щоб вимкнути контроль облікових записів користувачів: запустити всіх адміністраторів у режимі затвердження адміністратором.

Тож основні кроки для запуску технології Safeguard for Privileged Passwords [7]:

**Крок 1.** Створіть адміністратора авторизатора

**Крок 2.** Адміністратор авторизатора створює адміністраторів. Ось основні види адміністраторів:

1. Адміністратор користувачів
2. Адміністратор служби підтримки
3. Адміністратор пристрою
4. Адміністратор операцій
5. Аудитор
6. Адміністратор активів
7. Адміністратор політики безпеки

**Крок 3.** Адміністратор пристрою налаштовує пристрій:

1. IP адрес
2. Масу мережі
3. Шлюз по замовчуванню
4. DNS-сервера
5. DNS-суфікси

Налаштуйте параметри зовнішньої інтеграції, які застосовуються.

*Електронна пошта*: налаштуйте SMTP-сервер, який буде використовуватися для повідомлень електронною поштою. Safeguard for Privileged Passwords надає стандартні шаблони електронної пошти для більшості подій, які можна налаштувати.

*Ідентифікація та автентифікація:* налаштуйте служби каталогів, такі як сервери Active Directory та LDAP, для використання як постачальників

ідентифікації та автентифікації для користувачів Safeguard for Privileged Passwords . Налаштуйте Safeguard для привілейованих паролів як сторону, що перевіряє та використовує SAML 2.0 для інтеграції із зовнішніми службами для аутентифікації користувачів. Створіть сервер RADIUS, який буде використовуватися як первинний або вторинний провайдер аутентифікації.

*SNMP:* налаштуйте SNMP для надсилання пасток SNMP на консоль SNMP, коли виникають певні події.

Starling: Приєднуйтесь до Safeguard for Privileged Passwords to Starling, щоб скористатися іншими послугами Starling, такими як двофакторна автентифікація Starling.

*Системний журнал:* налаштуйте сервери системного журналу, на які потрібно надсилати повідомлення про події.

**Крок 4.** Адміністратор користувачів додає користувачів

1. Увійдіть у настільний клієнт, використовуючи обліковий запис адміністратора користувачів.
2. Додайте користувачів, які можуть увійти до Safeguard for Privileged Passwords.
3. Надайте дозволи адміністратора служби підтримки одному або декільком користувачам.

**Крок 5.** Адміністратор активів додає керовані системи

1. Увійдіть у настільний клієнт за допомогою облікового запису адміністратора активів.
2. Додайте розділи та, за бажанням, делегуйте право володіння розділами іншим користувачам (Додати розділ ).
3. Задайте за необхідністю наступні параметри керування паролями (або відредагуйте правила та параметри за промовчанням, визначені при додаванні розділу):

Правила використання пароля облікового запису

Зміна паролю

Перевірити пароль

Групи синхронізації паролів

4. Встановіть такі параметри керування ключами SSH за необхідністю:

Змінити налаштування ключа SSH

Перевірте налаштування ключа SSH

Відкрийте для себе налаштування ключа SSH

Установки груп синхронізації ключів SSH

5. (Необов'язково) Створіть профілі або відредагуйте створені профілі за замовчуванням ( Створення профілю пароля ).

6. Додайте ресурси у відповідні розділи та профілі ( Додавання активу (настільний клієнт)).

7. Додайте облікові записи для керування доступом до активів ( Додавання облікового запису ).

**Крок 6.** Адміністратор політики безпеки додає політики запитів на доступ

1. Увійдіть у настільний клієнт за допомогою облікового запису адміністратора політики безпеки.

2. Встановіть причини. ( Налаштування | Запит на доступ | Причини )

3. Налаштувати твердження де завгодно. ( Налаштування | Зовнішня інтеграція | Твердження де завгодно ).

4. Додати групи користувачів (Додати групи користувачів).

5. Додавання локальних користувачів або користувачів каталогу до локальних груп користувачів ( Додавання користувачів до групи користувачів ).

6. Додати групи облікових записів ( Додати групу облікових записів ).

7. Додати облікові записи до груп облікових записів (додавання одного або декількох облікових записів до групи облікових записів).

8. Додати права ( Додавання права ).

9. Додавання користувачів або груп користувачів до прав ( Додавання користувачів або груп користувачів до прав ).

10. Створення політик запитів на доступ (Створення політики запитів на доступ).

Відповідно до розкритих кроків технології налаштування Safeguard for Privileged Passwords покажемо реалізацію налаштування користувача у модулі SPP.

Технологія створення користувача в модулі SPP:

Наступним кроком буде створення нового користувача: Вкладка *Identity* (Ідентифікація). На рис.3.3 показано форму «New User» (Новий користувач) на вкладці Identity. Адміністратор заповнює основні дані користувача:

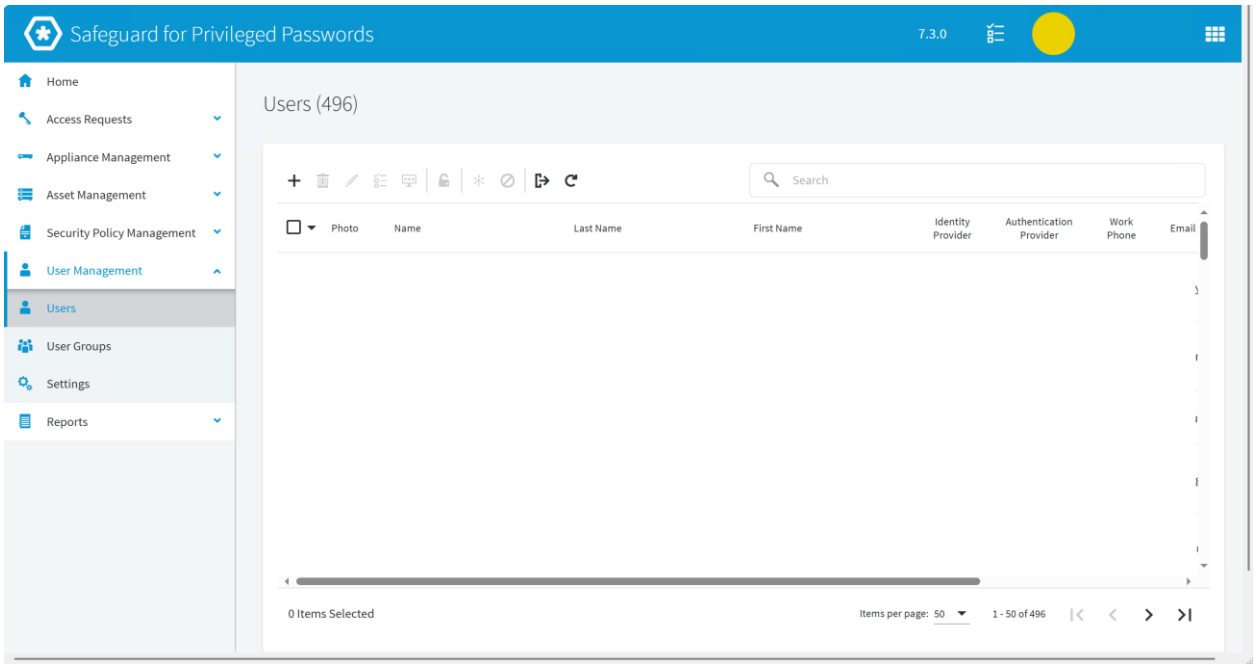


Рис.3.2. Головне вікно модуля SPP для створення користувача в модулі SPP

Identity Provider (Постачальник ідентифікації) встановлено як Local (Локальний).

Username (Ім'я користувача) (обов'язкове), First Name (Ім'я), Last Name (Прізвище), Work Phone (Робочий телефон), Mobile Phone (Мобільний телефон), Email (Електронна пошта), Description (Опис).

Time Zone (Часовий пояс): Вибрано «(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius».

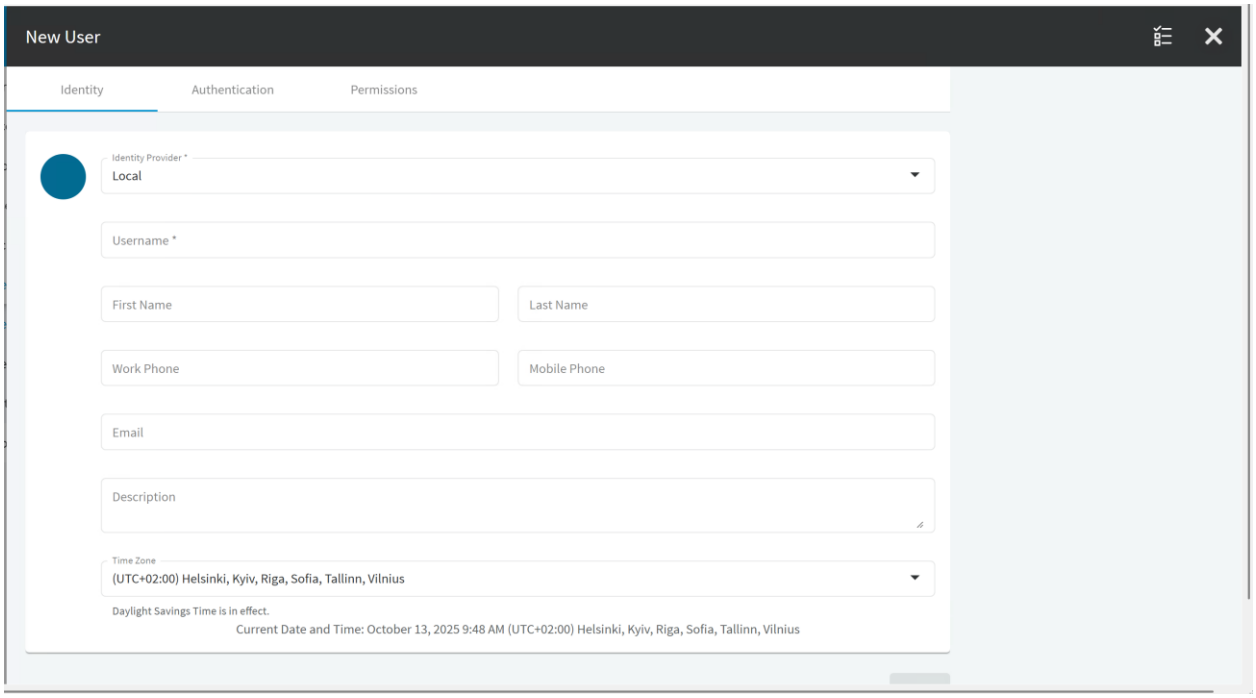


Рис. 3.3. Форма заповнення «New User»

Наступним кроком є заповнення вкладки Authentication (Автентифікація), яку забражено на рис.3.4. Тут налаштовуються параметри входу:

Authentication Provider (Постачальник автентифікації): Встановлено як Local.

Login Name (Ім'я для входу) (обов'язкове).

Password (Пароль) (обов'язкове), яке має відповідати вимогам: 8-64 символи, дозвіл на повторювані символи, принаймні одна велика літера, одна мала літера та одна цифра.

Параметри прапорців: Password Never Expires (Пароль ніколи не закінчується), User Must Change Password at Next Login (Користувач повинен змінити пароль при наступному вході), Require Secondary Authentication (Вимагати вторинної автентифікації).

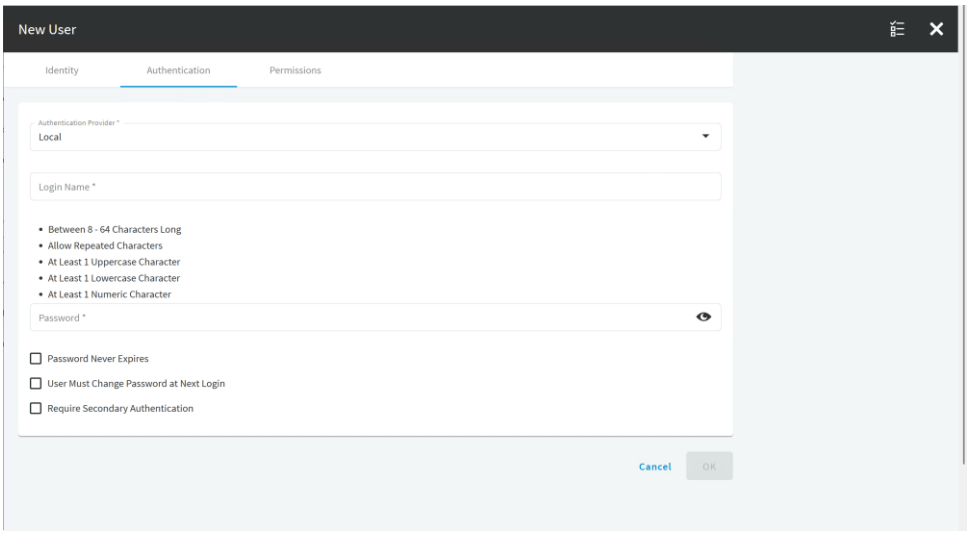


Рис.3.4. Вкладка Authentication

Надалі необхідно заповнити вкладку Permissions (Дозволи), яке зображено на рис.3.5. Тут адміністратор призначає користувачеві ролі та дозволи, такі як Authorizer (Авторизатор), User (Користувач), Help Desk (Служба підтримки), Appliance (Пристрій), Operations (Операції), Auditor (Аудитор), Application Auditor (Аудитор застосунків), System Auditor (Системний аудитор), Asset (Об'єкт), Security Policy (Політика безпеки) та Personal Password Vault (Персональне сховище паролів).

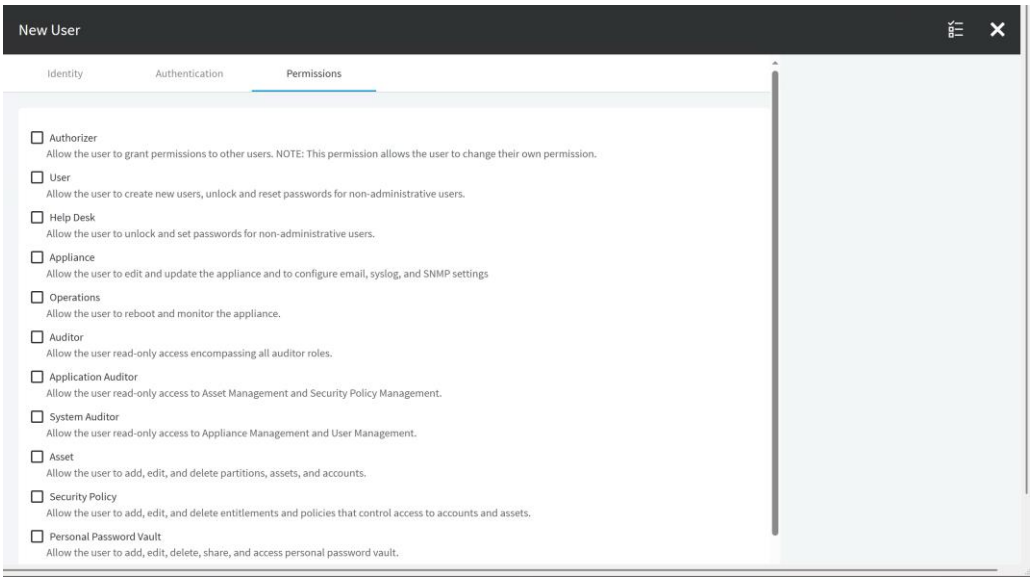


Рис. 3.5. Вкладка Permissions

Після завершення процедури заповнення основних вкладок щодо відомостей користувача, не обхідно перейти до наступного кроку «Створення прав для користувача» (рис.3.6).

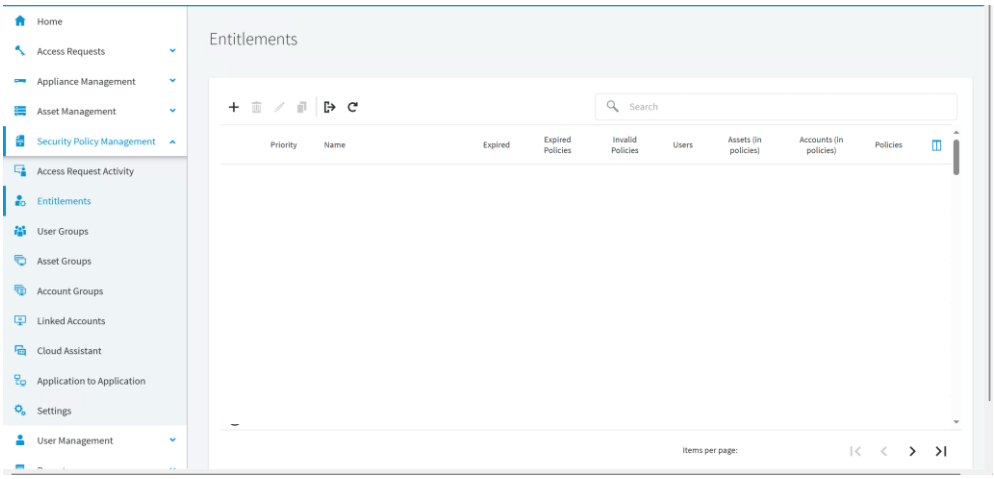


Рис.3.6. Створення прав для користувача

«Створення прав для користувача» демонструє процес створення та налаштування права доступу (Entitlement) і пов'язаної з ним політики запиту доступу (Access Request Policy). Адміністратор переходить до розділу Entitlements (Права доступу) в Security Policy Management (Керування політиками безпеки).

Тут створюється нове право доступу (New Entitlement) з Name (Ім'ям) (наприклад, "tst"), Description (Описом) та Priority (Пріоритетом). Також можна налаштувати термін дії права доступу (Have the Entitlement Expire on Date and Time) та використання часових вікон (Use Time Windows).

Про створенні нової політики необхідно в розділі політики в новому вікні надати назву політики, для прикладу на рис.3.7 назва нової політики «tst».

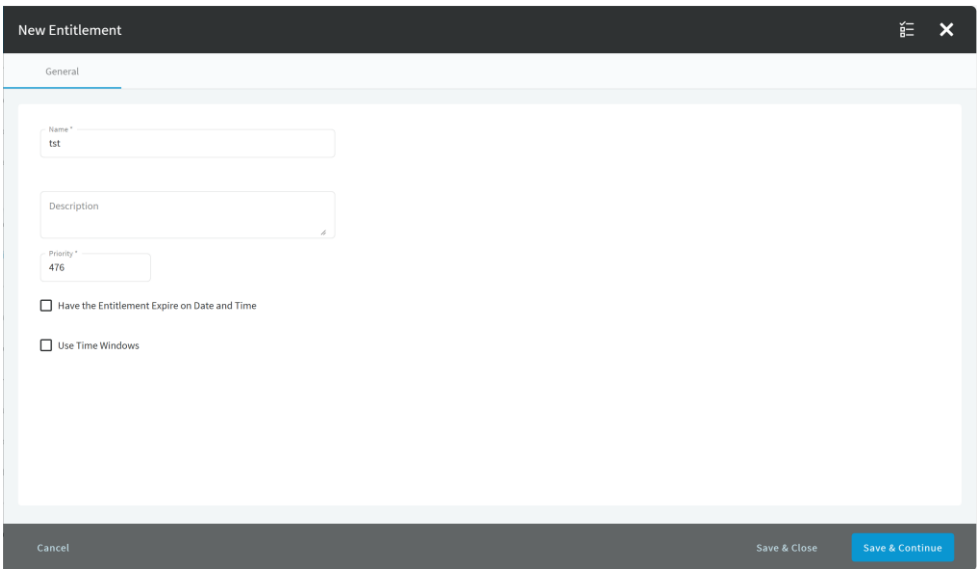


Рис.3.7. Створення нової політики

Після цього починається процес створення політики для обраного користувача (рис 3.8).

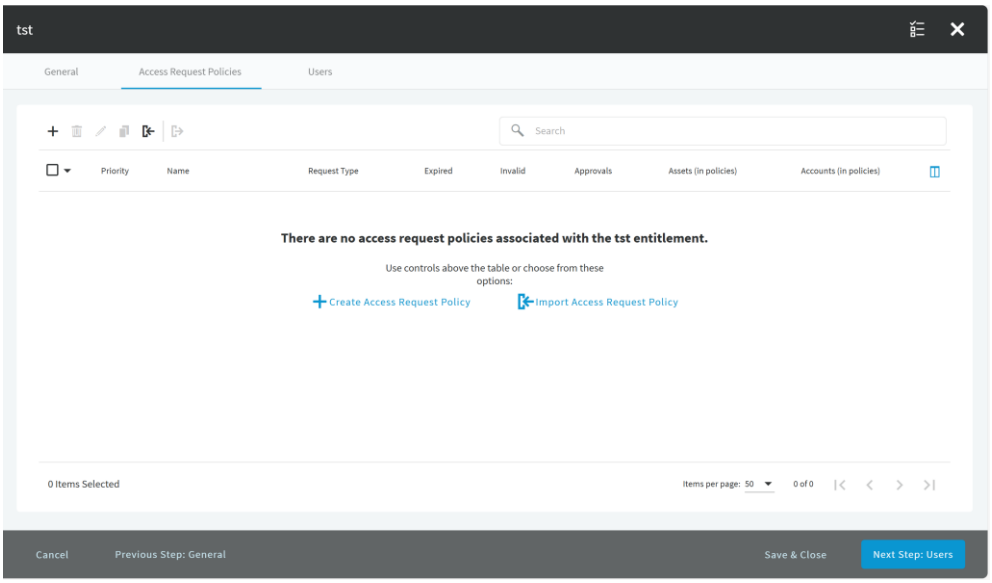


Рис.3.8. Початок створення політики для нового користувача

На рис.3.9. налаштовується яким чином користувач буде отримувати доступ до сесії. Наприклад через пароль або  RDP.

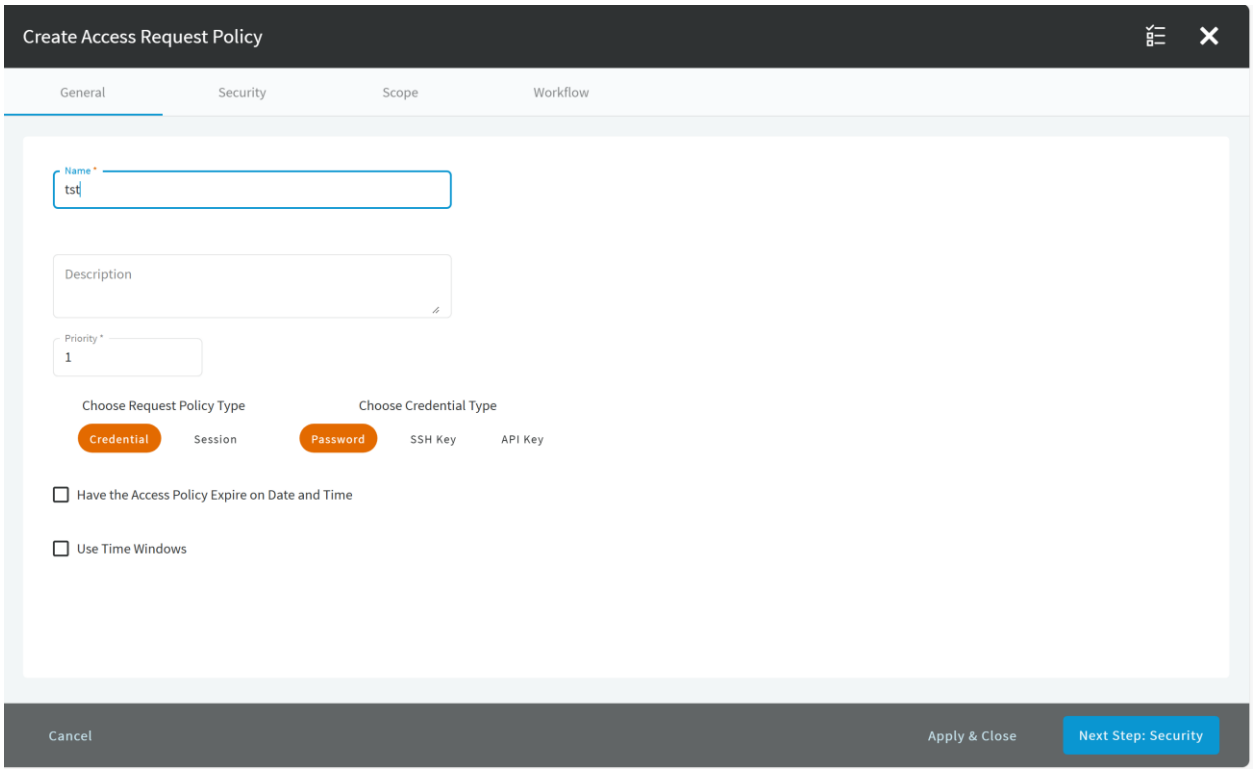


Рис.3.9. Налаштування шляху доступу користувачеві

У вкладці Security (рис.3.10) виконуються налаштування щодо зміни паролю для сесій користувача.

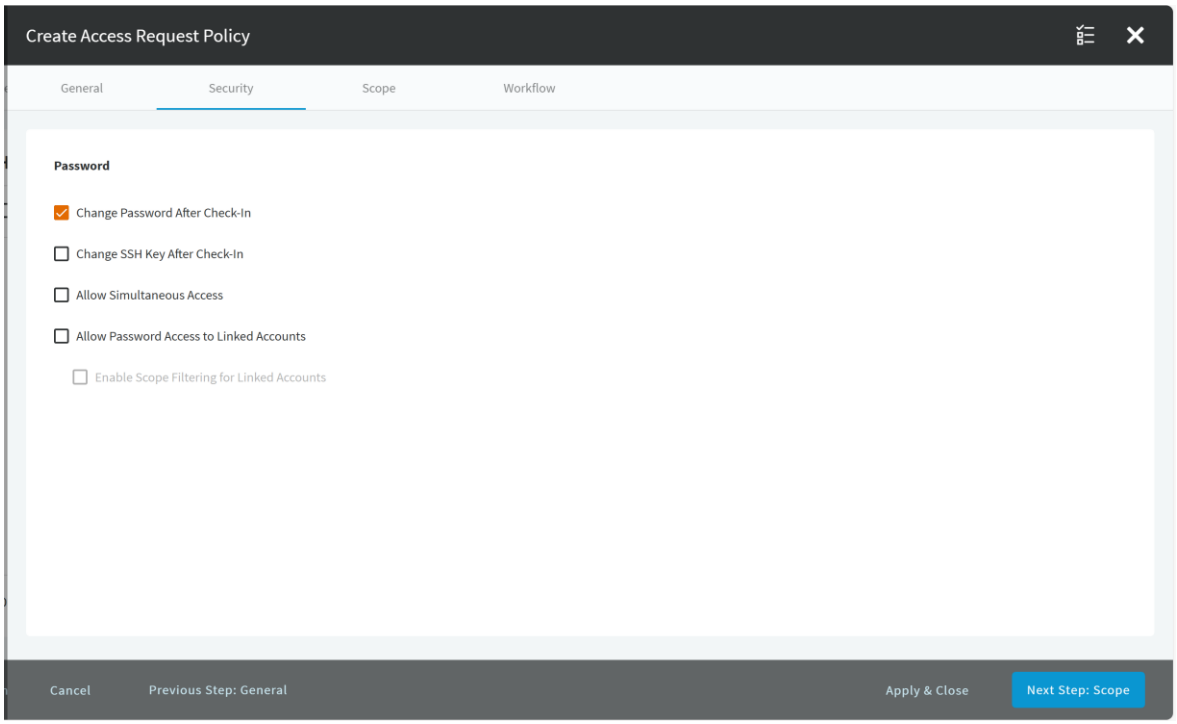


Рис.3.10. Налаштування зміни паролю

Даля адміністратор переходить до розділу Scope. У розділі Scope (рис.3.11) надається можливість надання доступу користувачу до певних вже створених об’єктів.

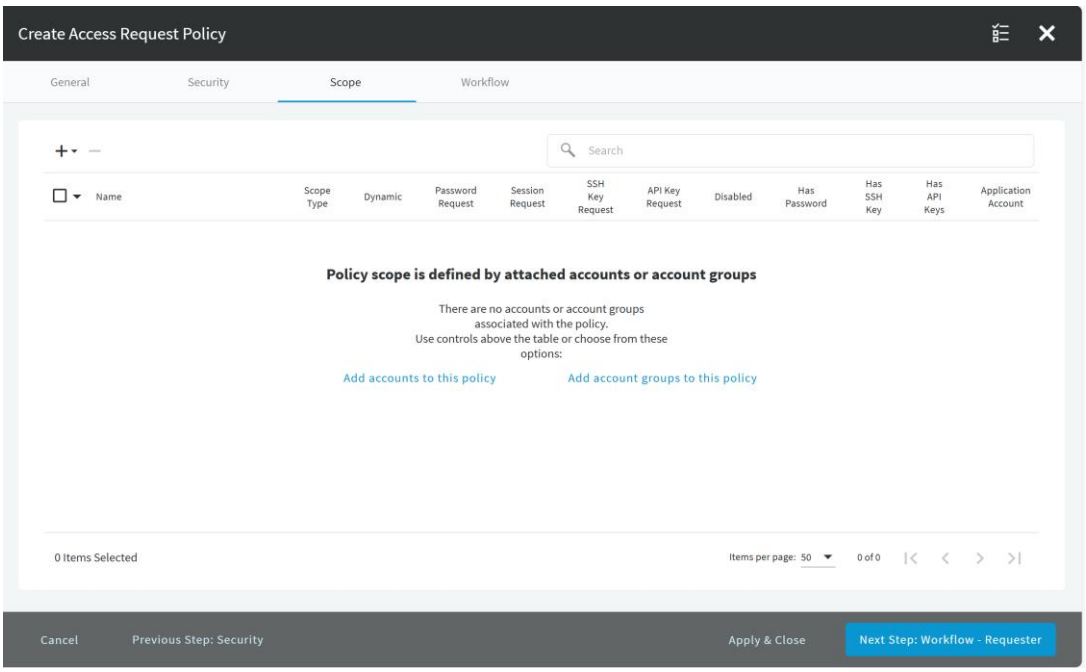


Рис.3.11. Розділ Scope

Наступний розділ, який налаштовує адміністратор є Workflow. У розділі Workflow (рис.3.12) задаються параметри, які обмежують час сесії користувача та надають можливість виклику екстренної сесії, в разі, коли користувачу необхідно надати доступ до об’єкту в неробочий час. Тут можна додати адміністраторів системи, які будуть отримувати повідомлення, щодо кожної екстренно викликаної сесії.

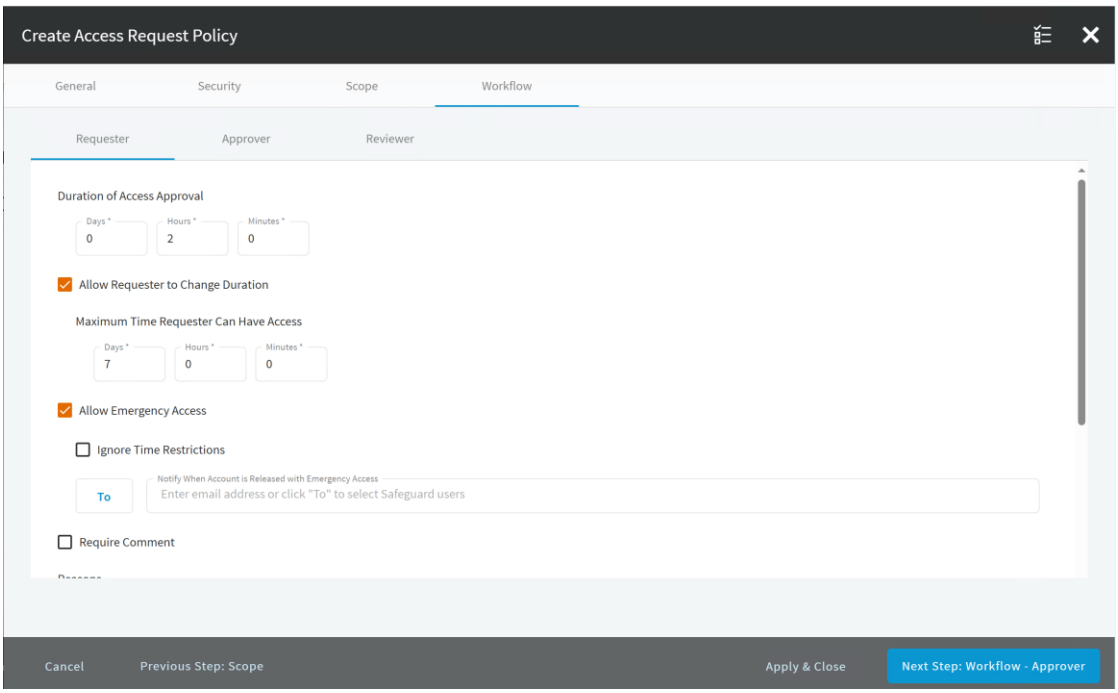


Рис 3.12. Розділі Workflow

Останнім кроком для налаштування користувача – є налаштування відповідних доступів до об’єктів (рис.3.13) Об’єктом може бути сервер.

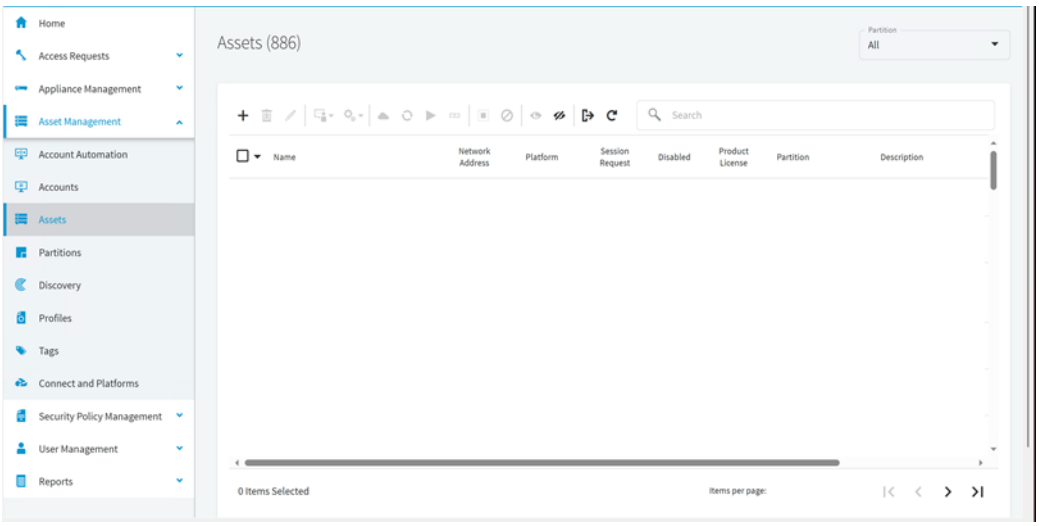


Рис.3.13. Налаштування доступів до об’єктів

У розділі для створюється об’єкт, до якого користувач зможе отримати доступ, у вигляді сесії. В залежності від обраної системи необхідно заповнити дані обраного об’єкту.

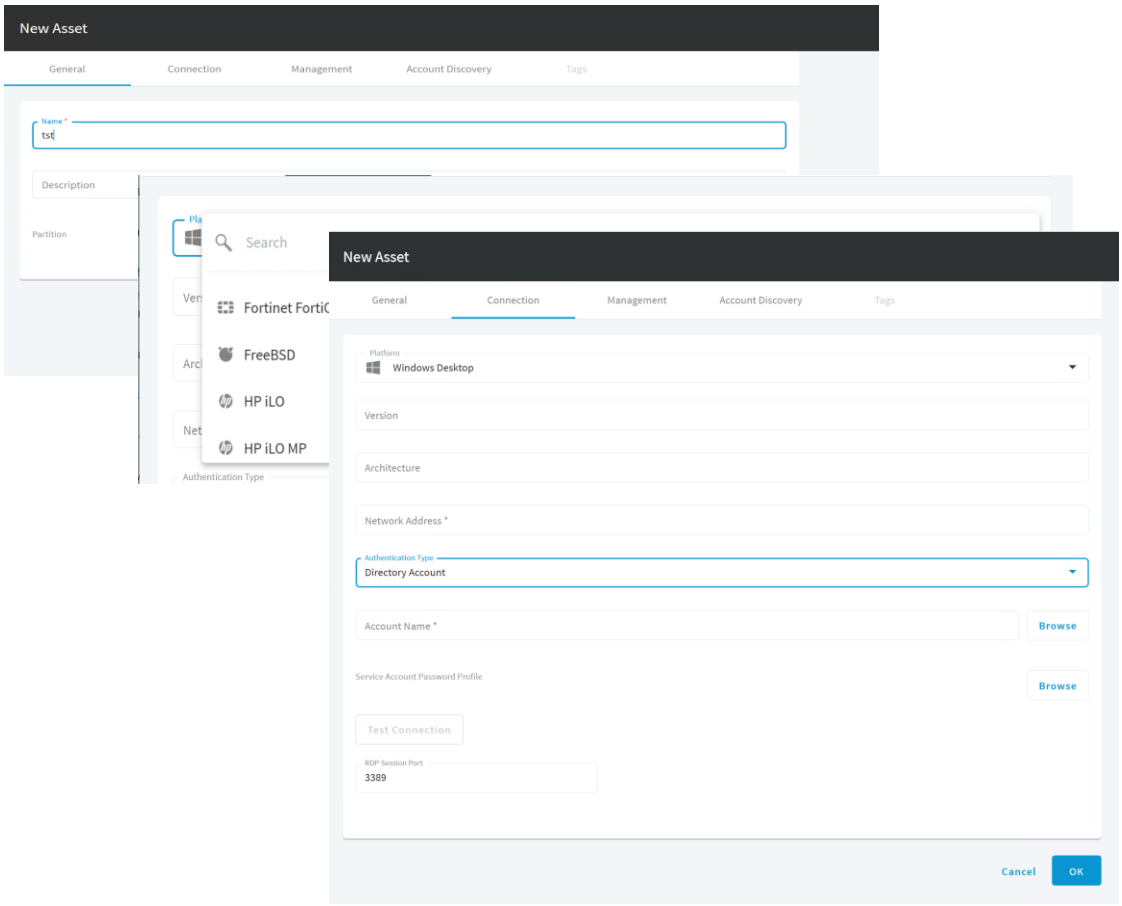


Рис.3.14. Створення об’єкту

Надалі, після всіх налаштувань, адміністратор має закріпити за користувачем створену політику та додати політики до об’єкту.

## 3.2. Розробка загальних рекомендацій щодо захисту привілейованих даних користувачів

У сучасних інформаційних систем організації управління привілейованим доступом (PAM) є не просто елементом безпеки, а стратегічне значення захисту критично важливих активів організації. Чим більш цілісними та послідовними будуть політики безпеки та дотримання привілеїв в організації, тим вища її здатність оперативно та ефективно реагувати на внутрішні та зовнішні загрози, а

також успішно виконувати численні вимоги відповідності. Привілейовані облікові записи, що мають високий рівень доступу до систем, баз даних та мережевого обладнання, є основною мішенню для кіберзлочинців. Тому комплексне впровадження PAM є критично важливим для мінімізації ризику несанкціонованого доступу та зловживання правами.

Для побудови надійної системи захисту привілейованого доступу та облікових записів, організації повинні керуватися низкою ключових рекомендацій.

*1. Встановлення політики та чітке визначення привілеїв*

Першочерговим кроком є встановлення та застосування формальної політики управління привілеями. Ця політика повинна чітко визначати порядок надання, використання та скасування привілейованого доступу. Жоден привілейований обліковий запис не повинен бути поза контролем. Необхідно визначити та взяти під контроль усі такі облікові записи, включаючи ті, що використовуються постачальниками, підрядниками, базами даних, програмами, службами та навіть обліковими записами у соціальних мережах, які мають адміністративний контроль над корпоративними ресурсами. Складання повного списку всіх активних привілейованих облікових записів у мережі є безперервним процесом, який вимагає оновлення при кожному створенні чи зміні облікового запису.

2. *Застосування принципу найменших привілеїв*

Принцип найменших привілеїв є центральним елементом PAM. Його суть полягає в тому, щоб забезпечити мінімальну кількість привілеїв, необхідних для виконання конкретних завдань. Цей принцип застосовується до кінцевих користувачів, кінцевих точок, програм, служб та систем. Важливо обмежити кількість людей з привілейованими обліковими записами до якомога меншого кола осіб. Крім того, кожен привілейований обліковий запис повинен мати точно налаштовані привілеї, що мінімізує потенційний збиток у разі його компрометації.

*3. Управління доступом Just-in-Time (JIT) та підвищення привілеїв*

Для додаткового зменшення ризиків слід використовувати підхід Just-in-Time (JIT). Організації повинні підвищувати привілеї в міру необхідності лише для конкретних додатків та завдань, і лише в той момент, коли вони потрібні. Це

означає, що як тільки діяльність завершена, привілеї мають бути негайно скасовані. Цей механізм вимагає застосування спеціалізованої технології для контрольованого підвищення та зниження привілеїв. Крім того, системи та мережі, що вимагають більш високих рівнів довіри, повинні реалізовувати більш надійні засоби контролю безпеки, відповідно до їхньої важливості.

*4. Посилення автентифікації та захист облікових даних*

Забезпечення надійної автентифікації є життєво важливим. Потрібно використовувати надійні паролі, які здатні протистояти поширеним атакам (таким як перебір або словникові атаки) і регулярно їх змінювати. Для найбільш конфіденційних привілейованих доступів рекомендується використовувати одноразові паролі. Застосування автентифікації єдиного входу (SSO) допомагає приховати фактичні паролі від користувачів та процесів. У контексті вразливостей слід забезпечити доступ з мінімальними привілеями на основі оцінки вразливостей, що дозволить автоматично обмежувати привілеї та запобігати небезпечним операціям.

*5. Моніторинг, аудит та усвідомлення ризиків*

Ефективний PAM включає постійний контроль. Організації повинні увімкнути базові показники для дій привілейованих користувачів та збирати інші дані про ризики. Це забезпечує більше уявлення про ризики привілеїв. Всі операції з ідентифікацією, такі як вхід, використання спільних паролів, спроби доступу та дії скидання, повинні підлягати аудиту. Моніторинг та запис усіх сеансів привілейованих користувачів у режимі реального часу є необхідним для виявлення підозрілої активності та проведення розслідувань.

Впровадження спеціалізованих рішень PAM надає організації значні операційні переваги та підвищує рівень кіберзахисту.

# ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні наукові результати:

Визначено поняття привілейованого доступу. Згідно передбачених законів, постанов та стандартами, такими як GDPR, ISO 27001, PCI DSS, HIPAA, SOX, FIPS, NIST було визначено, що для захисту інформаційної системи існують вказівки як забезпечити захист привілейованих даних користувачів.

Визначено що PAM є одним з головних механізмів забезпечення безпеки доступу до інформаційної системи і вважається багатьма аналітиками одним з найбільш важливих проектів безпеки для зниження ризиків.

Проаналізовано загрози та приклади атак для отримання привілейованих даних користувачів інформаційної системи організації, а також підходи щодо їх усунення.

Проаналізовано та обрано технологію привілейованого захисту користувачів інформаційної системи організації на прикладі технології One Identity Safeguard.

Визначено функції основних модулів, які входять до архітектури системи One Identity Safeguard привілейованого доступу користувачів інформаційної системи організації.

На основі отриманих результатів розроблено варіант технології розгортання та налаштування рішення One Identity Safeguard привілейованого доступу користувачів інформаційної системи організації для модуля SPP.

В результаті виконання роботи надано рекомендації фахівцям з кібербезпеки щодо управління привілейованими даними користувачів інформаційної системи організації.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Morey J. Haber, Darran Roll Identity Attack Vectors: Implementing an Effective Identity and Access. - 2020. 200p.

2. Привілейований доступ. URL: https://cloudnetworks.ru/analitika/chto-takoe-pam/ .

3. Функційні можливості PAM [Електронний ресурс] – Режим доступу: https://safe-surf.ru/specialists/article/5281/660685/ .

4. Привылейовані облыковы записи. URL: https://www.kv.by/blog/users/softline/1061251-krazha-privilegirovannyh-zapisei-vy-v-bezopasnosti .

5. Звіт Gartner; Магічний квадрант управління привілейованим доступом URL: https://www.gartner.com/doc/reprints?id=1-26UE4193&ct=210719&st=sb]/ .

6. Витоки даних. URL: https://securis.com/news/privileged-access-management/ .

7. Вартість витоків. URL: https://www.ibm.com/reports/data-breach .

8. Gartner PAM. URL: https://www.beyondtrust.com/blog/entry/gartner-pam-magic-quadrant .

9. Роль првілейованого доступу. URL: https://eska.global/blog/rol-upravlinnya-privilejovanim-dostupom-pam-u-vidpovidnosti-vimogam-standartiv-bezpeki-compliance .

10. ISO/IEC 27001:2022Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/ru/standard/27001.

11. Payment Card Industry Data Security Standard (PCI DSS) URL: https://www.pcisecuritystandards.org/standards/ .

12. Петухова М.О., Мазур А.Т. Технологія управління привілейованим доступом: порівняння рішень. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С. 21-23.