ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНОГО ДОСТУПУ ПРАЦІВНИКІВ ДО КОРПОРАТИВНИХ СИСТЕМ ОРГАНІЗАЦІЙ НА БАЗІ РІШЕННЯ THYCOTIC SECRET SERVER»

Виконала студентка 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Парфенюк Т.М.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Привілейовані користувачі, тобто співробітники або підрядники з адміністративним доступом до IT-систем компанії, становлять найбільшу загрозу для безпеки організації. Маючи привілейований доступ до перегляду, зміни чи видалення конфіденційних даних або адміністрування критично важливих систем, ці користувачі володіють обліковими даними для входу. Саме це створює вразливість для витоку даних за межі компанії, навіть у тому випадку, коли слабких місць всередині мережі немає.

Саме тому безперечно важливим є потурбуватись, яким чином прівелейовані користувачі отримують доступ до корпоративних систем а також як саме вони подяться із даними, які необхідіні для входу до корпоративних систем.

Об'єкт дослідження – прівелейовані облікові записи.

Предмет дослідження – рішення для організації доступу прівелейованих облікових записів до ресурсів компанії.

Мета роботи – розробка рекомендацій щодо використання рішення для організації безпечного доступу до корпоративних ресурсів.

Завдання бакалаврської роботи:

– дослідити поняття облікового запису та прівелейованого облікового запису;

– ознайомитись із різними рішеннями для управління прівелейованими записами;

– дослідити функціональні можливості рішень PAM;

– розробити рекомендації щодо впровадження та використання рішення Thycotic Secret Server.

Методи дослідження – опрацювання технічної літератури за темою, аналіз технічної документації, проведення тестування інструментів, порівняльний аналіз сервісів.

Практичне значення одержаних результатів – рекомендації щодо розгортання та використання рішень для організації прівелейованих облікових

записів можуть бути використані у сфері забезпечення кібербезпеки у персональних та корпоративних інформаційних системах.

1 АНАЛІЗ НЕОБХІДНОСТІ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

1.1 Визначення поняття облікового запису та їх типів

Обліковий запис - це набір облікових даних, який дозволяє користувачеві отримати доступ до комп'ютерної системи, мережі або онлайн-сервісу [1]. Обліковий запис використовується для ідентифікації та автентифікації користувача, а також для контролю доступу до системних ресурсів і даних [2].

Коли користувач виконує вхід до комп'ютера або мережі, він вказує ім'я користувача та пароль, пов'язані з його обліковим записом. Після цього система перевіряє облікові дані і надає доступ до ресурсів і даних, до яких користувач має право доступу на основі своїх дозволів і привілеїв.

Облікові записи використовуються для того, щоб дозволити окремим користувачам змінювати свої налаштування та уподобання в системі, наприклад, фон робочого столу, заставки та налаштування додатків. Облікові записи також можна використовувати для відстеження активності користувачів та аудиту використання системи з метою забезпечення безпеки та дотримання нормативних вимог.

Окрім облікових записів окремих користувачів, існують також облікові записи системного рівня, які використовуються для виконання системних функцій, таких як запуск системних служб і фонових завдань. Ці облікові записи зазвичай створюються під час налаштування системи і використовуються системними адміністраторами для управління та обслуговування системи.

У комп'ютерних системах та мережах існує декілька основних типів облікових записів, зокрема:

Облікові записи користувачів. Це індивідуальні облікові записи, які використовуються користувачами для доступу до комп'ютерної системи або мережі. Обліковим записам користувачів зазвичай призначаються дозволи та

привілеї, які визначають, до яких ресурсів і даних вони можуть отримати доступ і які дії вони можуть виконувати в системі.

Облікові записи адміністраторів. Це привілейовані облікові записи, які мають підвищені дозволи та доступ до функцій і ресурсів системного рівня. Облікові записи адміністратора використовуються системними адміністраторами та іншим уповноваженим персоналом для управління та обслуговування системи [1].

Службові облікові записи. Це облікові записи, які використовуються системними службами та фоновими завданнями для виконання автоматизованих функцій у системі [3].

Гостьові облікові записи. Це облікові записи, які надають обмежений доступ до системи користувачам, які не мають власних облікових записів. Гостьові облікові записи зазвичай мають обмежені дозволи та доступ до ресурсів і даних у системі.

Спільні облікові записи. Це облікові записи, які використовуються спільно кількома користувачами, наприклад, облікові записи, що використовуються командами або відділами для доступу до спільних ресурсів і даних. Спільні облікові записи можуть становити ризики для безпеки, оскільки може бути складно відстежувати та перевіряти дії, що виконуються за допомогою цих облікових записів [3].

Системні облікові записи. Це облікові записи, які створюються під час налаштування системи і використовуються операційною системою для виконання функцій системного рівня. Системні облікові записи зазвичай не використовуються окремими користувачами і не пов'язані з конкретною особою чи групою осіб [3].

Загалом, тип облікового запису залежить від ролі користувача та рівня доступу, необхідного для виконання його посадових обов'язків. Важливо керувати та захищати кожен тип облікового запису, щоб забезпечити безпеку та цілісність системи та даних.

1.2 Визначення поняття привілейованого користувача

Привілейовані облікові записи зазвичай використовуються для управління інфраструктурою, як службові облікові записи або для підключення додатків один до одного. Вони зустрічаються майже в кожному екземплярі IT-інфраструктури, мережевих пристроях, програмному забезпеченні та додатках в організації. Привілейовані облікові записи поширені в організаціях будь-якого розміру, оскільки вони абсолютно необхідні IT-відділу для підтримки роботи. Вони також потрібні зловмисникам і зловмисним інсайдерам, щоб успішно завершити атаку, не будучи зупиненими рішеннями безпеки [4].

Оскільки привілейовані облікові записи завжди надають доступ до інформації або об'єктів, які є цінними або критично важливими для діяльності компанії, вони потребують особливої уваги аудиту та управління.

Існує багато видів привілейованих облікових записів:

Облікові записи root та адміністратора зазвичай використовуються для встановлення та видалення програмного забезпечення та зміни конфігурацій. Вони надають дуже широкі та найвищі привілеї доступу до певних серверів або баз даних і також називаються обліковими записами суперкористувачів.

У Windows облікові записи адміністратора - це облікові записи користувачів, які використовуються для керування окремими аспектами комп'ютера, домену або всієї IT-інфраструктури підприємства.

Облікові записи адміністратора часто називають *Адміністратор* на окремих комп'ютерах і в невеликих середовищах. Однак, будь-який користувач у Windows може стати адміністратором, додавши його до відповідної групи.

Поширеними підтипами облікових записів адміністратора є локальний адміністратор і адміністратор домену.

Облікові записи адміністратора домену надають повний доступ і контроль над доменом Active Directory (AD). Ці облікові записи є особливо озброєними і небезпечними, оскільки вони дають контроль над усіма контролерами домену, робочими станціями домену і серверами-членами домену, а також дозволяють

змінювати конфігурацію Active Directory або будь-який вміст, що зберігається в Active Directory. Це включає створення нових користувачів, видалення користувачів і зміну їхніх дозволів [5].

Адміністратор домену - це різновид Адміністратор облікового запису.

Облікові записи локального адміністратора - це облікові записи користувачів, які можуть керувати локальним комп'ютером у Windows. Як правило, локальний адміністратор може робити все, що завгодно на локальному комп'ютері, але не може змінювати інформацію в активному каталозі для інших комп'ютерів та інших користувачів [2].

Обліковий запис локального адміністратора часто називають Адміністратор, але будь-який користувач може стати локальним адміністратором, додавши його до групи Локальний адміністратор.

Облікові записи служб використовуються для запуску процесів, таких як веб-сервери, сервери баз даних і сервери додатків. Облікові записи служб також можуть бути створені просто для зберігання даних і конфігураційних файлів.

Облікові записи служб не призначено для використання людьми, окрім як для виконання адміністративних операцій.

Облікові записи додатків пов'язані з конкретним прикладним програмним забезпеченням і зазвичай призначені для адміністрування, конфігурування або керування доступом до прикладного програмного забезпечення. Облікові записи додатків дозволяють взаємодіяти між додатками і зазвичай запускаються автоматично без участі людини. Винятком є завдання з обслуговування, що виконуються привілейованими користувачами.

Системні облікові записи створюються операційною системою під час інсталяції і використовуються для запуску компонентів операційної системи та керування пов'язаними з ними файлами [5].

Системні облікові записи часто мають попередньо визначені ідентифікатори користувачів. Прикладом системних облікових записів є обліковий запис root у Linux.

Різниця між системними та службовими обліковими записами іноді розмита. Багато системних облікових записів запускають процеси операційної системи, і в цьому відношенні вони схожі на службові. Деякі системні облікові записи, такі як root також використовуються системними адміністраторами.

1.3 Потенційні вразливості облікових записів

Організації можуть бути мати наступні вразливості у привілейованих облікових записах у межах компанії:

Надмірне надання привілеїв. Іншими словами, занадто багато користувачів мають надмірний доступ до корпоративних систем. IT-адміністратори зазвичай надають кінцевим користувачам надмірно широкий набір привілеїв. У випадку з комп'ютерами під управлінням Windows, користувачі часто входять в систему з правами адміністративного облікового запису. Якщо обліковий запис скомпрометований, зловмисник може використати будь-які привілеї, притаманні цьому обліковому запису.

Недостатня обізнаність про привілейовані облікові записи. Невідомі привілеї та некеровані привілейовані акаунти створюють небезпечні лазівки для зловмисників, у тому числі для колишніх співробітників, які залишили компанію, але зберегли доступ. Облікові записи додатків і служб часто залишаються поза увагою. Ці облікові записи можуть автоматично запускати привілейовані процеси для виконання дій, а також для зв'язку з іншими додатками, службами, ресурсами тощо.

Вбудовані облікові дані. Додатки, системи, мережеві пристрої та пристрої Інтернету речей зазвичай мають вбудовані облікові дані та/або дані за замовчуванням. Ці облікові дані можуть повторно використовуватися на багатьох подібних пристроях. Часто паролі добре відомі кіберзлочинцям і можуть бути легко вгадані. Крім того, розробники, члени DevOps-команди та інші користувачі часто кодують секретні дані у вигляді відкритого тексту в скриптах, кодах або файлах, щоб мати до них легкий доступ у разі потреби.

Спільні облікові записи адміністраторів. Спільне використання привілейованих облікових даних є поширеною практикою серед IT-команд, але це ускладнює, якщо не унеможливлює, відстеження привілейованих дій, виконаних через обліковий запис однією особою, що створює проблеми з безпекою, аудитом та дотриманням нормативних вимог [3].

Неефективні практики управління паролями в компанії. З тисячами і мільйонами привілейованих облікових даних, розкиданих по системах (Windows, Mac, Unix, Linux) і гібридних середовищах, людські процеси погано пристосовані до масштабування. Люди часто вдаються до небезпечних ярликів (наприклад, повторне використання паролів або SSH-ключів на різних серверах, активах та облікових записах, або зберігання паролів у документах, електронних таблицях чи коді), що може призвести до масштабної компрометації [4].

Використання безкоштовних, непідтримуваних інструментів, таких як sudo. Багато інструментів, таких як sudo, надають достатньо функціональності, щоб дозволити невеликим організаціям "впоратися" з адмініструванням. Однак, часто ці інструменти мають серйозні недоліки, які стають все більш очевидними зі збільшенням складності та масштабу. Не потрібно багато, щоб перерости sudo. Окрім того, що sudo забирає багато часу і є складним у використанні, йому бракує моніторингу цілісності файлів, безпеки журналів і можливостей централізованого керування. Це ключові недоліки, особливо якщо врахувати, що цей інструмент використовується в середовищах Unix/Linux, які, ймовірно, є найбільш чутливими системами і активами організації.

Сторонній постачальник/віддалений доступ. Незалежно від того, чи працюють співробітники компанії віддалено, чи сторонні постачальники - віддалений доступ відкриває небезпечні шляхи атак і є одним з найскладніших завдань кібербезпеки. VPN часто використовуються, але не надають детальних засобів управління привілеями.

1.4 Рекомендації щодо контролю доступу до систем на основі стандарту ISO 27001

Необхідно розробити, задокументувати та переглянути політику контролю доступу з відповідними бізнес-вимогами та вимогами інформаційної безпеки [6].

Керівництво з впровадження - власники активів повинні встановити відповідні правила контролю доступу, права доступу та обмеження для певних ролей користувачів до своїх активів, з урахуванням критичності інформації та суворості контролю, що відображає відповідні ризики інформаційній безпеці. Контроль доступу є як логічним, так і практичним, тому їх слід розглядати разом. Користувачам та постачальникам послуг слід надати чіткий, прозорий опис бізнес-вимог, яким мають відповідати засоби контролю доступу.

Політика інформаційної безпеки компанії повинна враховувати:

1. Вимоги безпеки, що застосовуються до додатків, які впливають на бізнес процеси;
2. Процедури авторизації та розповсюдження інформації, наприклад, концепцію необхідності знати рівень доступу до інформації, а також класифікацію інформації;
3. Узгодженість між правами доступу та політикою класифікації інформаційних систем та мереж;
4. Звернення до відповідного законодавства та інші договірні зобов'язання, що стосуються інформації або контролю доступу до інформації;
5. Управління правами доступу в розподілених та мережевих середовищах, яке розпізнає типи доступних з'єднань;
6. Розмежування функцій управління доступом, наприклад, запит на доступ, авторизація доступу, адміністрування доступу;
7. Формальні вимоги до авторизації для додатків доступу;
8. Вимоги до періодичного перегляду прав доступу;
9. Видалення прав доступу;

10. Архівування деталей всіх важливих інцидентів, пов'язаних з використанням та управлінням ідентифікаційними даними користувачів та секретною інформацією про автентифікацію [7].

1.5 Аналіз статистики інцидентів, пов’язаних із обліковими записами

Згідно зі звітом Verizon Data Breach Incident Incident Report за 2021 рік, облікові дані є найбільш затребуваним типом даних при порушенні безпеки.

Identity Defined Security Alliance повідомляє, що 79% організацій зіткнулися з порушенням безпеки, пов'язаним з ідентифікаційними даними.

Identity Theft Resource Center повідомляє, що кількість атак з використанням програм-вимагачів подвоїлася в 2021 році і, за прогнозами, випередить фішинг як основну причину компрометації даних у 2022 році [8].

Однак, що може стати несподіванкою, так це те, що не всі організації мають достатній рівень розуміння ризиків, пов'язаних з ідентифікаційними даними. Компанія Illusive на власні очі побачила ці «сліпі зони», працюючи з численними командами безпеки у секторах фінансових послуг, охорони здоров'я та роздрібної торгівлі (серед інших), які часто мають найдосконаліші програми безпеки. Протягом останніх 12 місяців була проведена робота з аналізу їхніх ідентифікаційних ризиків, результати якої представлено у звіті «Аналіз ідентифікаційних ризиків (AIR) 2022». Привілейовані користувачі мають надзвичайну владу у організації. Вони можуть скидати паролі, змінювати політики, встановлювати програмне забезпечення, витягувати або шифрувати дані.

Коли зловмисник компрометує кінцеву точку з одним із цих привілейованих ідентифікаторів, це схоже на гру з чит-кодами - він може робити майже все, що завгодно. Ризики, пов'язані з експлуатованими обліковими записами, дозволяють зловмисникам отримати початковий доступ, закріпитися в мережі, підвищити свої привілеї, обійти захист. На жаль, дослідження Illusive показує, що всі організації є вразливими і що 1 з 6 кінцевих точок має принаймні один ризик використання ідентифікаційних даних (рис. 1.1). Це дослідження розглядає ці ризики в трьох

вимірах: некеровані ризики облікових записів, неправильно зконфігуровані облікові записи та вразливі ризики облікових записів. Багато з цих ризиків перетинаються один з одним, і реальність така, що Illusive знаходить приклади некерованих, неправильно налаштованих і вразливих ідентифікаційних ризиків у кожній організації [8].

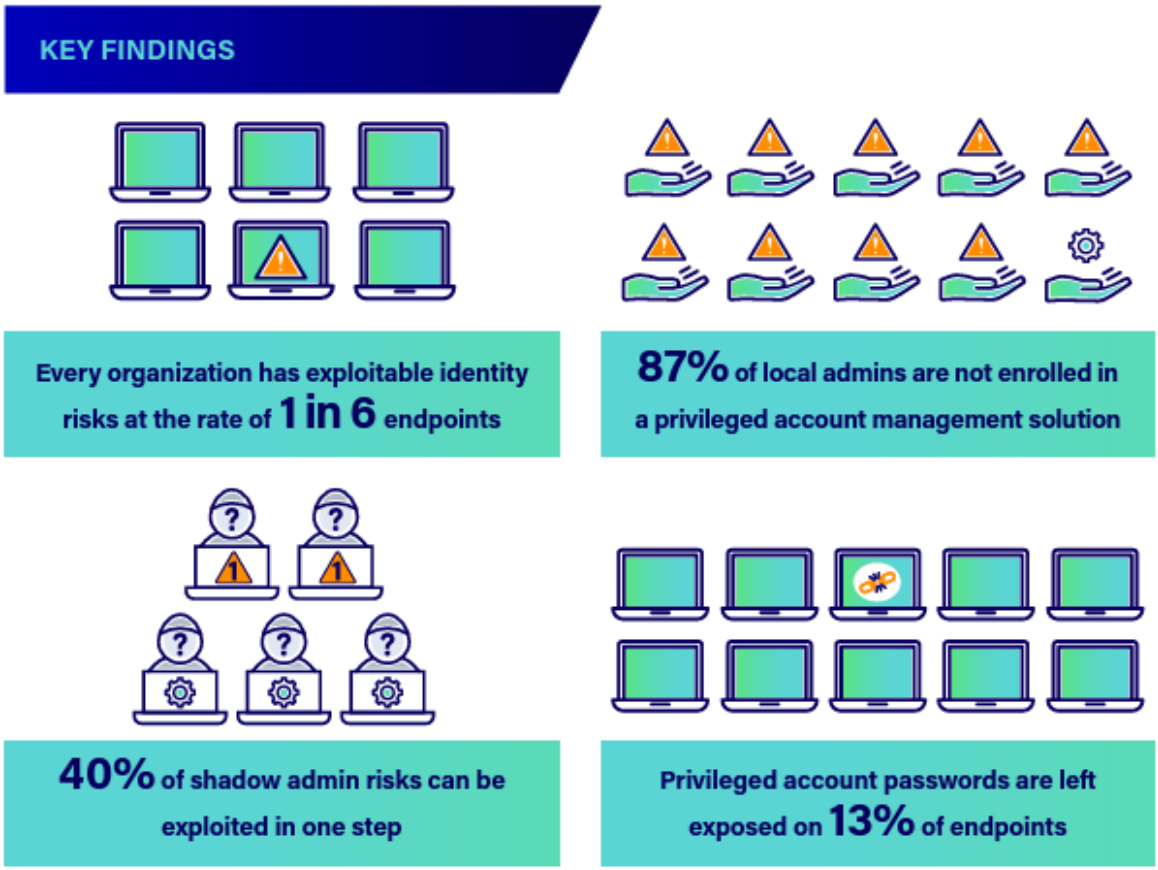

Рис. 1.1. Звіт Verizon Data Breach Incident Incident Report

Ризики, пов'язані з неправильним налаштуванням ідентифікаційних даних отримали назву «shadow admins». Подібно до того, як тіньові IT визначаються розгортанням IT-систем за межами видимості IT-адміністраторів, тіньові адміністратори визначаються користувачами з дозволами, які не є видимими для IT-адміністраторів - дозволами, які можуть бути використані для ескалації привілеїв. Під час аналізу ризиків для ідентичності Illusive виявила приклади неправильно налаштованих тіньових адміністраторів у всіх організаціях.

Наприклад, в одному випадку з медичною організацією Illusive виявила працівника служби підтримки 1-го рівня, відповідального за скидання паролів, який також мав дозвіл 3-го рівня на додавання адміністраторів домену. Якщо цей обліковий запис адміністратора рівня 1 був скомпрометований, зловмисник міг додати свій обліковий запис в якості адміністратора домену, щоб підвищити свої привілеї. Найважливіше те, що 40% ризиків тіньових адміністраторів можуть бути використані в один крок - якщо зловмисник скомпрометує один з цих неправильно налаштованих облікових записів, йому знадобиться лише одне право, наприклад, скинути пароль адміністратора домену, щоб підвищити свої привілеї до рівня адміністратора домену. Це легка здобич для зловмисників - її легко знайти і легко використати.

Також вагомим ризиком, хоча він спостерігається рідше, є тіньові адміністратори, які можуть захопити весь домен - якщо привілейовані ідентифікатори вважати ключами до королівства, то вони є королями цього королівства. Якщо зловмисник скомпрометує одного з таких тіньових адміністраторів, він мало що не зможе зробити. Найбільший ризик, хоча і спостерігається набагато рідше, становлять тіньові адміністратори з дозволами DCSync Microsoft Active Directory (1,7% тіньових адміністраторів мають дозволи DCSync). Дозволи DCSync, по суті, є перлиною організації - вони надають можливість копіювати контролер домену для створення нового або для синхронізації між двома контролерами. Це найвищий рівень дозволів.

Ще один ризик, на який слід звернути увагу, полягає в тому, що 1 з 50 тіньових адміністраторів є звичайним користувачем. Це ризик, оскільки вони ще більше віддалені від управління IT (інші тіньові адміністратори можуть принаймні бути зареєстровані в рішеннях для управління привілейованими обліковими записами). Це можуть бути користувачі, які починали свою кар'єру в IT-відділі і були переведені на нову посаду, користувачі, яких випадково додали до привілейованих груп, користувачі, яким тимчасово надали дозволи і забули про них, або користувачі, які були створені з абсолютно несподіваних джерел. Наприклад, в одному випадку з інтернет-магазином Illusive виявив тіньового

адміністратора на ім'я «Стів Роджерс». Якщо це ім'я здається знайомим, то це тому, що це альтер-его Капітана Америки. Коли цю знахідку було досліджено, то було виявлено, що всі Месники (наприклад, Тоні Старк, Брюс Беннер і т.д.) були присутні як тіньові адміністратори. Виявляється, ці тіньові адміністратори були створені червоною командою під час тесту на проникнення, але не були видалені після завершення тесту. Вони існували в Active Directory більше двох років, поки не були виявлені Illusive [8].

Крім того, 41% вразливих облікових даних привілейованих облікових записів доменів Windows належать тіньовим адміністраторам. Це ще більший ризик, оскільки тіньові адміністратори, як правило, невідомі, а це означає, що інші засоби контролю безпеки не будуть налаштовані на них, що дозволить атакам на них залишатися невиявленими довше. Це не лише ілюструє, як ці ризики для ідентичності можуть перетинатися, але й те, як організації намагаються отримати інформацію про них. Досить погано, що тіньові адміністратори уникають виявлення існуючими рішеннями для управління обліковими записами, але їхнє викриття означає, що вони активно використовуються. Організації дійсно «не знають, чого вони не знають», коли мова йде про ці ризики.

Кожна організація вразлива до некерованих, неправильно налаштованих та вразливих ідентифікаційних ризиків. Кількість облікових записів, якими організаціям доводиться керувати, різко зросла, оскільки бізнес покладається на все більшу кількість систем і додатків. Крім того, постійна зміна ідентичностей та автентифікацій для підтримки бізнесу призвела до значних складнощів як в управлінні, так і в захисті ідентичностей. В епоху, коли зловмисники використовують ідентифікаційні дані як основний вектор атаки, навіть короткий доступ до привілейованих ідентифікаційних даних несе значні ризики.

Висновки до першого розділу

Проаналізовано поняття «прівелейованого обліковаго запису» та ризиків, які пов’язані із цим поняттям. Прівелейованим обліковим записом є той, який може

надавати розширений доступ до ресурсів компанії. Саме тому даний тип облікових записів є особливо вразливим, оскільки отримавши прівелейований доступ до системи, зловмисники мають можливість виконувати будь-які дії без обмежень.

Досліджено вразливості облікових записів: надмірне надання привілеїв, вбудовані облікові дані, спільні облікові записи а також надання віддаленого доступу до ресурсів компанії.

2 ОПИС ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ РІШЕНЬ КЛАСУ PAM

2.1 Визначення рішень класу PAM

PAM (Privileged Access Management) – це рішення та процеси, які дозволяють IT-відділам керувати та проводити аудит діяльності всіх «привілейованих користувачів». Привілейований користувач має адміністративний доступ до критично важливих систем і даних [12]. Наприклад, особа, яка має право створювати та видаляти облікові записи електронної пошти на сервері Microsoft Exchange Server, є привілейованим користувачем. Як і будь-які інші привілеї, привілеї «root» слід надавати лише довіреним особам. PAM захищає організацію від випадкового або навмисного зловживання привілейованим доступом. З цієї причини PAM має займати чільне місце у впровадженні ISO 27001. СУІБ повинна відстежувати співробітників та підрядників, а також віддалених або навіть автоматизованих користувачів. Деякі привілейовані користувачі можуть навіть обійти існуючі протоколи безпеки. Якщо адміністратори можуть вносити несанкціоновані зміни в систему, отримувати доступ до заборонених даних, а потім приховувати свої дії, це наражає організацію на серйозний ризик. У термінах ISO 27001, привілейований користувач може підірвати значну частину СУІБ, випадково або навмисно [7].

Privileged Access Management (PAM) - це автоматизоване рішення для керування паролями та сеансами, яке забезпечує безпечний контроль доступу, аудит, сповіщення та запис для будь-якого привілейованого облікового запису. Технологія призначена для управління локальним або спільним обліковим записом адміністратора домену; особистим обліковим записом користувача; обліковими записами служб, операційної системи, мережевих пристроїв, баз даних і додатків, і навіть ключами SSH, хмарою і соціальними мережами [3]. PAM дозволяє ефективно впроваджувати ISO 27001, пропонуючи безпечний, спрощений спосіб

авторизації та моніторингу всіх привілейованих користувачів для всіх відповідних систем. Зокрема, рішення даного класу:

- надає привілеї користувачам лише для тих систем, в яких вони авторизовані;

- надає доступ лише тоді, коли він потрібен, і відкликає доступ, коли потреба в ньому минає;

- уникає необхідності для привілейованих користувачів мати або потребувати локальні/прямі паролі;

- централізовано і швидко керує доступом до систем [14].

Рішення для керування привілейованим доступом відрізняються за архітектурою. Однак більшість з них пропонують наступні компоненти:

Керування доступом. Керує доступом до привілейованих облікових записів і створює єдину точку входу, що відповідає визначенню політики контролю доступу ISO 27001 та її впровадженню [6]. Привілейований користувач запитує доступ до системи через консоль рішення. Менеджер доступу знає, до яких систем користувач може отримати доступ і який рівень привілеїв він має. Супер-адміністратор може додавати/змінювати/видаляти облікові записи привілейованих користувачів у консолі, таким чином зменшуючи ризик того, що колишній працівник отримає доступ до критично важливої системи. Він також надає супер-адміністраторам централізований перегляд всієї історії сеансів привілейованих користувачів, реалізовуючи повну видимість і контроль над стратегічним обладнанням.

Керування паролями. Керування паролями - це функція безпеки, яка допомагає користувачеві зберігати та впорядковувати паролі. Вона запобігає тому, щоб привілейовані користувачі знали справжні паролі/облікові дані для доступу до критично важливих систем. Сховище паролів також може унеможливити ручну зміну паролів на фізичних пристроях - ризик, який усувається за допомогою засобів фізичного контролю. У цьому випадку система PAM зберігає паролі в безпечному сховищі і відкриває доступ до системи привілейованому користувачеві після того, як він або вона отримає дозвіл на доступ. Вона також може розширювати політику управління паролями адміністратора, впроваджуючи механізми захисту облікових

даних, такі як A2A PM (Application-to-Application-Password-Management), автоматична зміна паролів і т.д [15].

Керування сесіями. Модуль управління сеансами забезпечує моніторинг і запис усіх дій користувачів у режимі реального часу для запобігання інцидентам і проведення аналізу та аудиту записаних сесій.

Процес керування прівелейованимиоблікомим записами повинен складатись із наступних кроків:

Крок 1. Визначення існуючих прівелейованих облікових записів в компанії.

Крок 2. Введення багатофакторної автентифікації для співробітників. Які мають прівелейовані облікові записи, а також реєстрація облікових записів.

Крок 3. Запровадження рішення PAM, що включає в себе:

- Контроль на прівелейованим доступом до корпоративних систем;
- Автоматизовану зміну паролів за розкладом;
- Попередження адміністраторів безпеки про неправомірні дії;
- Логування всіх подій, пов’язаних із корпоративними системами, до яких співробітники мають доступ [15].

2.2 Характеристика рішення Thycotic Secret Server

Delinea Secret Server - це рішення для управління привілейованим доступом (PAM) корпоративного рівня, що допомагає організаціям захистити привілейовані облікові записи та організувати доступ до критично важливих систем і додатків, а також керувати ними. Рішення Delinea розроблені таким чином, щоб бути непомітними для користувачів, але при цьому простими у використанні для IT-команд і команд безпеки. Незалежно від того, чи працюють вони в хмарі або локально, рішення Delinea легко налаштовуються, масштабуються для зростання і є достатньо потужними, щоб захистити організацію незалежно від рівня зрілості PAM. Рішення було визначене лідером серед рішень PAM за версією Gartner Magic Quadrant 2022 (рис. 2.1), а також лідером за версією KuppingerCole (рис. 2.2) [13].

Рис. 2.1. Огляд вендорів від Gartner Magic Quadrant для рішень класу PAM

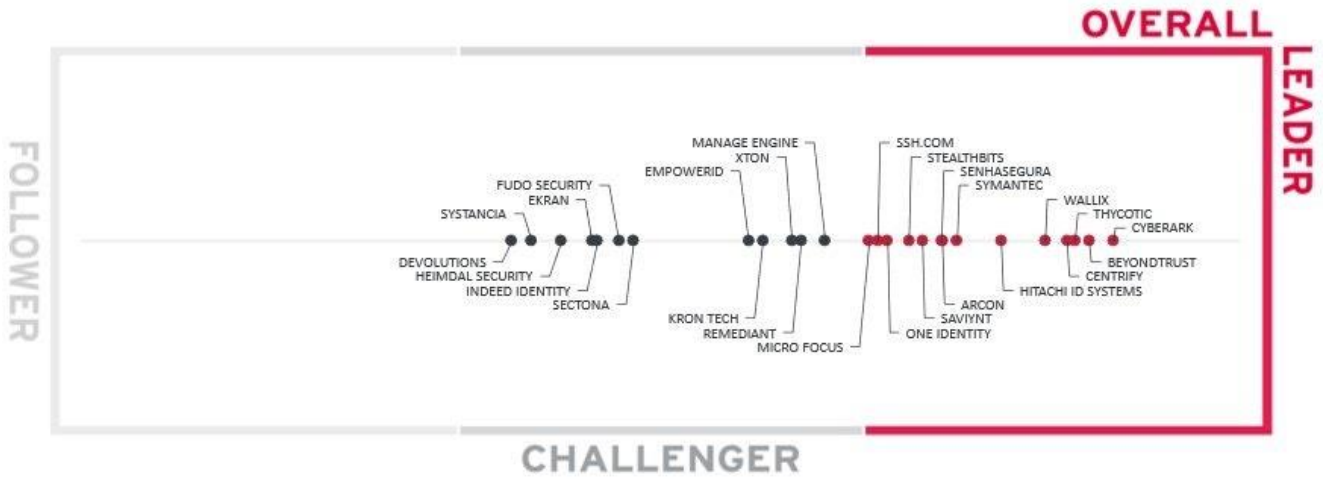

Рис. 2.2. Позиція Thycotic Secret Server в статистичному аналізі від KuppingerCole

Рішення Secret Server надає централізоване сховище для зберігання та управління обліковими даними привілейованих облікових записів, а також безпечний шлюз для доступу та управління привілейованими обліковими записами [11].

Secret Server можна встановити на фізичному сервері або віртуальній машині. Рішення має наступну архітектуру:

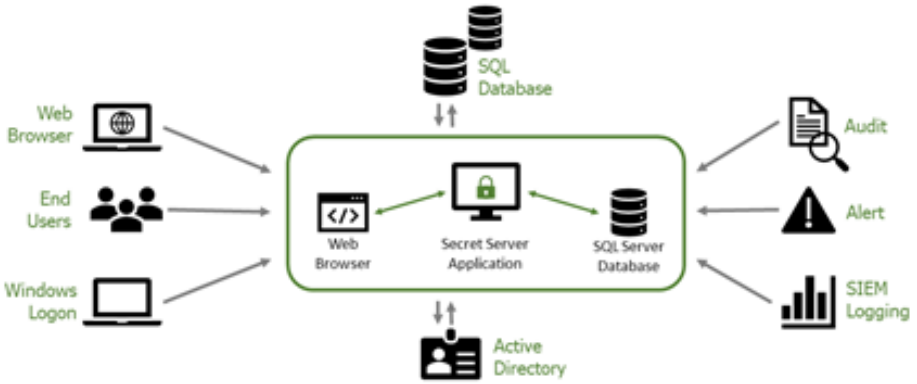

Рис. 2.3. Архітектура рішення Secret Server

Рішення Thycotic Secret Server містить наступний функціонал:

Secure Vault and Password Manager — забезпечує управління своєю інфраструктурою з єдиної консолі за рахунок використання багатофакторної аутентифікації та створення політик, які визначають рівні доступів для користувачів до secrets. Можливість створювати secrets з паролями та імпортувати їх з інший менеджерів паролів, для спрощення процедури переносу до Secret Server.

Access Control — контроль доступу дає змогу впроваджувати політику найменших привілеїв і керувати нею, згідно якої користувачі мають лише той доступ, який їм потрібен для виконання своїх посадових обов’язків. Наприклад, адміністратори можуть гарантувати, що користувачі не зможуть випадково чи навмисно змінити адміністративні налаштування, до яких вони не повинні мати прав [11].

Automation — використовуючи Secret Server, можна автоматизувати привілейовані зміни паролів за розкладом. Вбудовані графіки зміни паролів і терміну дії забезпечують автоматичну зміну критичних паролів без ручного втручання. Також можна задати вимоги до паролів, щоб вони відповідали корпоративним політикам. Автоматична перевірка облікових даних secrets через

встановлені проміжки часу дозволяє виявляти та сповіщати про зміни облікових даних поза Secret Server.

Discovery — Secret Server може сканувати мережу на наявність облікових записів локального адміністратора та завантажувати інформацію в безпечне сховище Secret Server. Наприклад, Secret Server може просканувати мережу, знайти кожен ноутбук, а потім взяти під контроль обліковий запис локального адміністратора, змінивши пароль (застосовуючи політику паролів вашої організації) і контролюючи майбутній доступ до цих облікових даних у сховищі Secret Server. Таке сканування також може бути проведене за допомогою скриптів PowerShell [11].

Session Monitoring & Control — за допомогою даного модуля, адміністратори в режимі реального часу можуть переглядати всі сесії, які були запущені з Secret Server. Окрім звичайного перегляду, є можливість робити записи сесій, переривати їх або надсилати користувачу повідомлення із запитанням, для чого він виконує ті чи інші дії.

Approval Workflow — робочий процес затвердження покращує видимість і відслідковування всіх привілейованих облікових записів, особливо тих, до яких звертаються для спеціальних проектів і треті сторони. Secret Server дає можливість створювати такі робочі процеси для запиту доступу до secrets, запиту коментаря або ж отримання доступу, використовуючи одноразовий пароль.

Disaster Recovery — Secret Server підтримує SQL AlwaysOn і Database Mirroring для створення резервної копії всіх збережених даних у реальному часі. Завдяки автоматичному переключенню після відмови, SQL Secret Server забезпечує високу доступність і резервування даних.

Кластеризація веб-серверів забезпечує як високу доступність, так і балансування навантаження, дозволяючи кільком веб-серверам запускати Secret Server. Кластерне середовище є ключовим у сценаріях аварійного відновлення, оскільки можна автоматично переключатися на окремий веб-сервер без простоїв. Крім того, продуктивність покращується завдяки балансуванню навантаження завдяки наявності кількох серверів, які одночасно обробляють запити.

Enhanced Auditing, Reporting and Compliance — Secret Server дає можливість адміністраторам консолі створювати аудиторські звіти, звіти про активність користувача в системі або про secrets, які були попередньо створені. Звіти можуть створюватись за розкладом або одноразово та бути використані для подальшого аналізу та усунення зауважень [11].

2.3 Характеристика рішення OneIdentity

One Identity пропонує рішення, які допомагають клієнтам підвищити операційну ефективність, зменшити ризики, контролювати витрати та посилити кібербезпеку.

Рішення One Identity Safegurd є провідним лідером у сфері PAM (рис. 2.4) [13].

Рис. 2.4. Позиція OneIdentity Safeguard в аналізі від Gartner Magic Quadrant для рішень класу PAM

Рішення містить наступні функціональні можливості:

1. Захист привілейованих паролів. One Identity Safeguard для привілейованих облікових записів автоматизує, контролює та захищає процес надання авторизаційних даних за допомогою управління доступом на основі ролей та автоматизованими робочими процесами. Крім того, рішення дозволяє керувати паролями з будь-якого місця і практично з будь-якого пристрою. Захист привілейованих сеансів.

За допомогою One Identity Safeguard для привілейованих сеансів можна контролювати, відстежувати та записувати привілейовані сеанси адміністраторів, підрядників та інших користувачів з високим рівнем ризику. Дії користувачів під час сеансів записуються, що полегшує пошук подій сеансів, допомагає спростити та автоматизувати звітність, а також полегшує аудит і дотримання вимогам. Крім того, Safeguard для привілейованих сеансів служить проксі-сервером і перевіряє трафік протоколу на рівні додатків на рівні додатків і може відхиляти будь-який трафік, що порушує протокол - таким чином, роблячи його ефективним протокол, що робить його ефективним захистом від атак.

2. Аналітика прівелейованих сеансів. За допомогою One Identity Safeguard для аналітики можна змусити аналітику поведінки користувачів працювати на вас, виявляючи раніше невідомі внутрішні та зовнішні загрози, а також виявляти та зупиняючи підозрілі дії. Аналітика оцінює рівень потенційного ризику загроз, щоб можна було розставити пріоритети у реагуванні, вжити негайних заходів щодо загроз і, зрештою, запобігти витоку даних.

3. Створення корпоративних політик. Використовуючи безпечний веб-браузер з підтримкою мобільних пристроїв, можна запитувати доступ і надавати схвалення для привілейованих паролів та сесії. Запити можуть бути схвалені автоматично або вимагати подвійного/багаторазового схвалення відповідно до політики організації. Політика може враховувати особу та рівень доступу запитувача, час і день спроби запиту, а також конкретний ресурс, який запитується - або все разом.

4. Повний аудит, запис і відтворення сеансів. Вся активність сеансу, включаючи натискання клавіш, переміщення миші і переглянуті вікна - фіксується, індексується і зберігається в захищених від несанкціонованого доступу журналах аудиту, які можна переглядати як відео та шукати, як у базі даних. Команди безпеки можуть шукати певні події в сеансах і відтворювати запис, починаючи з саме з того місця, де відбулася подія, що відповідає критеріям пошуку. Аудиторські сліди зашифровані, з позначкою часу та криптографічним підписом для цілей криміналістики та дотримання нормативних вимог.

5. Налаштування проксі шлюза. Safeguard для привілейованих сеансів можна розгорнути в режимі, що не вимагає змін у робочих процесах користувачів. Діючи як проксі-шлюз, Safeguard може працювати як невидимий для користувача і сервера. Адміністратори можуть продовжувати використовувати клієнтські програми, з якими вони знайомі і можуть отримувати доступ до цільових серверів і систем без будь-яких порушень у повсякденній роботі.

6. Аналіз поведінки користувачів. Кожен користувач має свій власний шаблон поведінки, навіть коли виконує ідентичні дії, такі як набір тексту або переміщення миші. Алгоритми, вбудовані в Safeguard для привілейованої аналітики, перевіряють ці поведінкові характеристики (перехоплені Safeguard для привілейованих сеансів). Динаміка натискання клавіш і аналіз руху миші допомагають виявити порушення, а також служать для безперервної біометричної автентифікації [10].

7. Власне сховище паролів. Усі співробітники компанії можуть зберігати та генерувати випадкові паролі для акаунтів у особистому сховищі паролів. Це дозволяє організації використовувати санкціонований інструмент з можливістю безпечного обміну та відновлення паролів, що забезпечує необхідний рівень безпеки та видимості бізнес-акаунтів.

Архітерктура рішення включає центральну консоль управління, систему перевірки та сервер для розгортання (рис. 2.3).

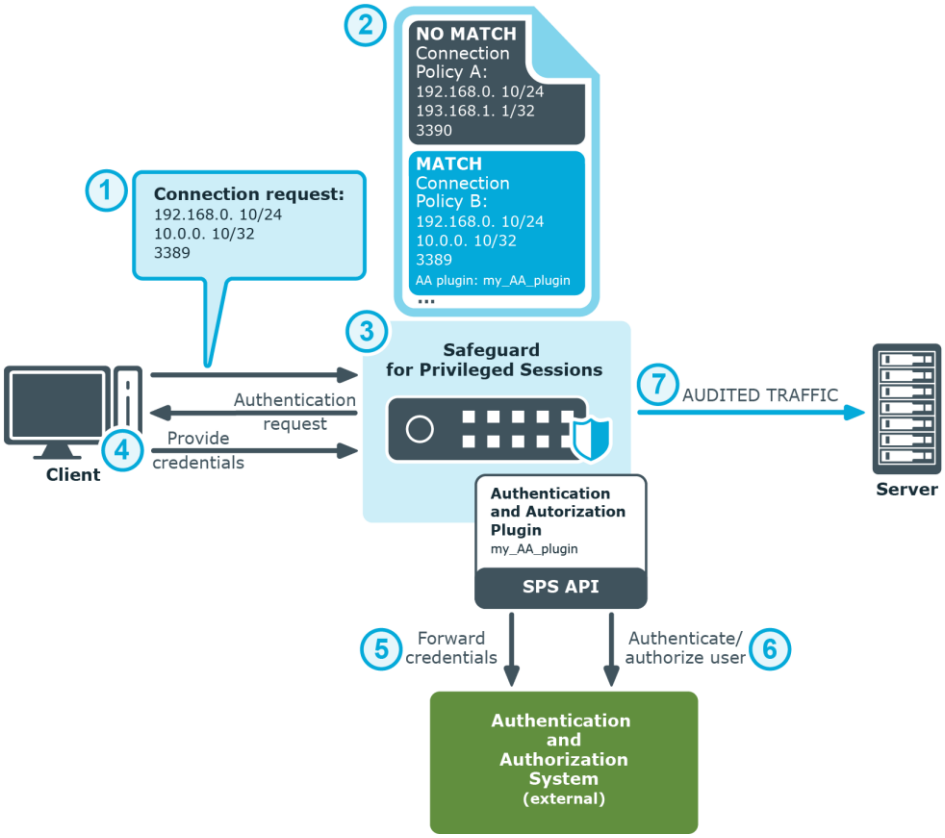

Рис. 2.5. Архітектура рішення OneIdentity Safeguard

Висновки до другого розділу

Досліджено рішення, що керують прівелейованими обліковими записами, що має на меті їх захист від викрадення або зміни.

Розглянуто два рішення: Thycotic Secret Server та OneIdentity Safeguard, які у своєму функціоналі містять наступне: контроль облікових записів, моніторинг сеансів, створення корпоративних політик, що є корисним для команд інформаційної безпеки.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ДОСТУПУ ДО СИСТЕМ КОМПАНІЇ НА БАЗІ РІШЕННЯ THYCOTIC SECRET SERVER

3.1 Принципи реалізації рішення класу PAM

Для впровадження рішення потрібно мати стратегію управління привілейованими обліковими записами (PAM), яка допоможе визначити, які типи функцій використовувати для різних облікових записів і конфіденційних даних, які будуть зберігати. Нижче наведено кілька рекомендацій щодо створення стратегічного плану.

Визначення даних в зоні ризику. Необхідно класифікувати всі типи конфіденційних даних, які потрібно надійно зберігати та керувати ними. Потрібно визначити де існують найбільші ризики та больові точки у поточній стратегії управління паролями. Важливо, що дані в зоні ризику часто включають не лише паролі [7].

Після визначення облікових записів, необхідно вирішити, хто буде використовувати PAM рішення для доступу та управління цими обліковими записами. Загальноприйнятим підходом є зосередження уваги на одній групі користувачів і паролях, які вони регулярно використовують, а потім розширення на інші команди, як тільки буде розроблена хороша стратегія.

Визначення рівнів привілеїв. Надання користувачеві доступу до облікового запису на Secret Server може передбачати різні рівні привілеїв. Потрібно визначитись, які дії будуть дозволені користувачеві: щоб користувач міг редагувати ім'я користувача, машину або пароль секрету, або тільки переглядати секрет, ділитися секретом з іншими користувачами.

Визначення вимог до паролів. Малоймовірно, що всі облікові записи матимуть однакові вимоги до складності паролів та графіку їхньої зміни.

Насправді, для кращої безпеки, слід мати певну варіативність. Можна створити набори вимог до паролів, щоб контролювати довжину, символи та складність паролів, а потім застосувати їх до різних типів акаунтів за допомогою секретних шаблонів. Шаблони секретних паролів також дозволяють встановити період дії за замовчуванням, який може означати, як часто пароль облікового запису буде автоматично змінюватися [7].

Оцінка наявних налаштувань. Переходячи до використання нового інструменту для керування паролями, важливо врахувати, як облікові записи використовуються у компанії.

3.2 Налаштування ролей в межах Secret Server

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

Ролі можна призначити декілька дозволів. Наприклад, можна призначити ролі права адміністрування користувачів, редагування секрету, власного секрету та перегляду Active Directory. Потім цю роль можна призначити користувачу або групі [11].

Щоб призначити ролі користувачу, необхідно натиснути кнопку **Assign Roles** на головній сторінці **Roles** (рис. 3.1). Залежно від того, яку вкладку вибрано, на цій сторінці можна переглянути ролі, призначені користувачам, або переглянути користувачів, яким призначено ролі. Щоб змінити ці налаштування, потрібно натиснути кнопку **Edit**. Тепер потрібно обрати роль зі списку та призначити або скасувати призначення користувачів ролі. На вкладці **By User or Group** можна вибрати користувача або групу зі списку та призначити або скасувати призначення їм ролей у полі списку для вибору.

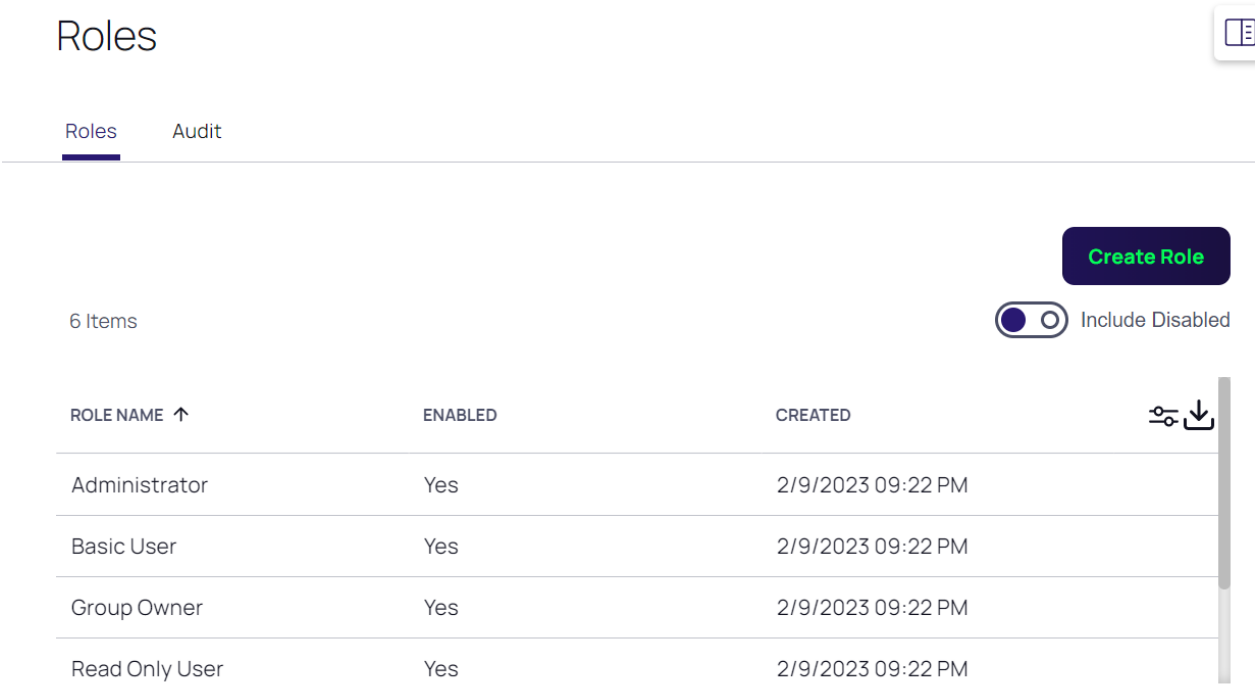

Рис. 3.1. Roles Dashboard

3.3 Додавання користувачів до консолі Secret Server

Після проведення інвентаризації в межах компанії, можна переходити до самого налаштування обраної системи.

Для того, щоб додати нового користувача до консолі необхідно відкрити меню **Users, Roles, Access** та обрати **User Management** (рис. 3.2).

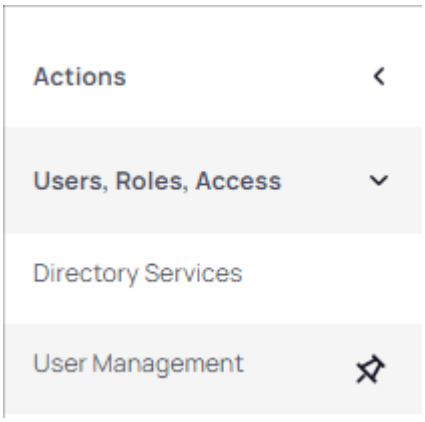

Рис. 3.2. Вибір вкладки, що дозволяє керувати користувачами у консолі

Для зміни налаштувань окремого користувача, потрібно натиснути на його ім’я в колонці User Name на сторінці Users (рис. 3.3). Пошук користувачів

здійснюється за допомогою рядка пошуку у верхній частині таблиці. Щоб показати користувачів, позначених як неактивні, потрібно встановити прапорець Show Inactive Users.

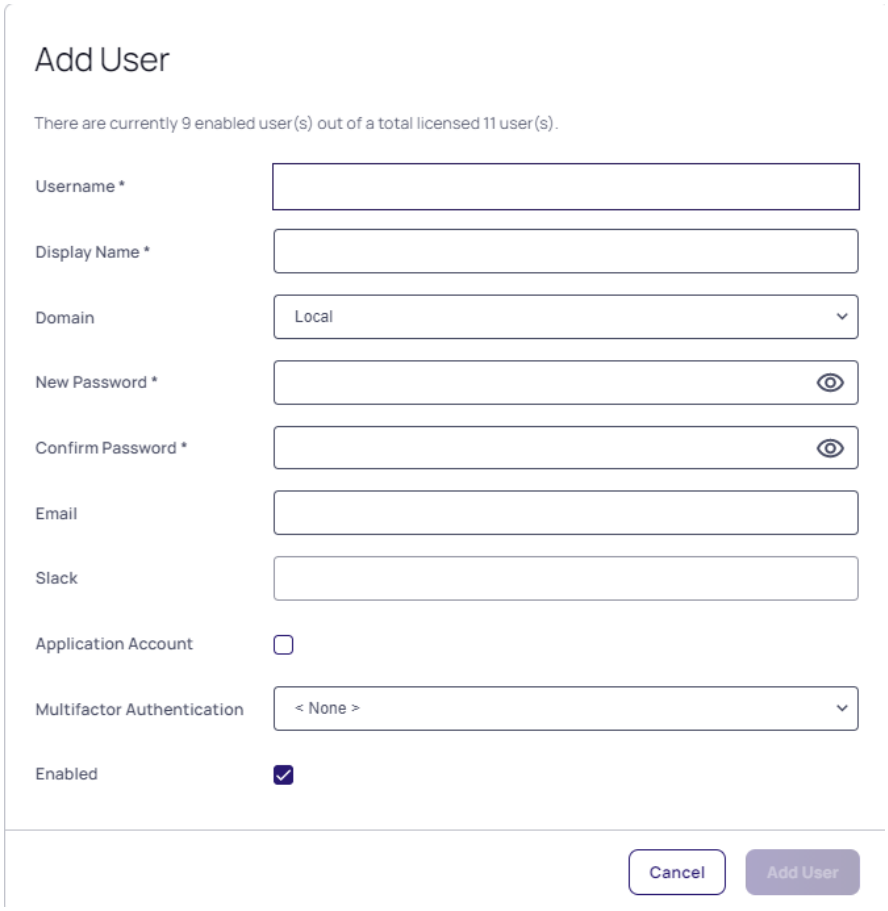

Рис. 3.3. Необхідні поля для заповнення, щоб додати нового користувача

3.4 Додавання нових облікових записів до консолі

Облікові записи, які були додані до консолі рішення мають назву секрети. Секрети охоплюють широкий спектр захищених даних, кожен тип яких представлений і створений за допомогою шаблону.

Для створення нового секрету, необхідно перейти у вкладку **Secrets** з бічної панелі консолі та натиснути **New Secret,** після чого можна обрати той тип даних, які необхідно зберігати (рис. 3.4):

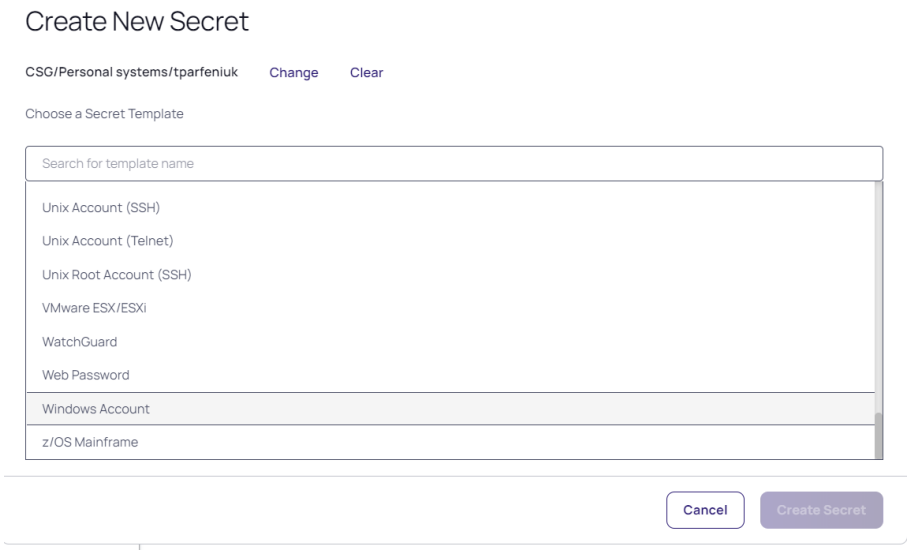

Рис. 3.4. Вибір необхідного шаблону для додавання нового секрету

Після вибоку шаблону для створення, з’явиться вікно із додатковими полями для заповнинння. В даному випадку ми оберемо RDP підключення, щоб мати можливість віддалено підключатись до систем (рис. 3.5):

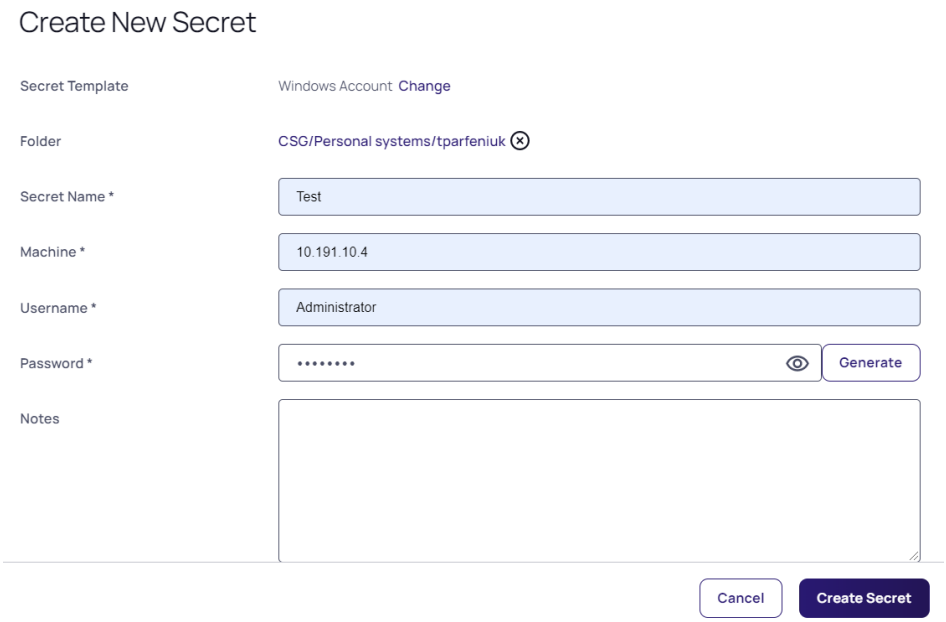

Рис. 3.5. Заповнення облікових даних для додавання нового секрету

Таким чином також створимо тестовий секрет для UNIX облікового запису, щоб мати можливість встановлювати SSH сесію за допомогою рішення Secret Server (рис. 3.6):

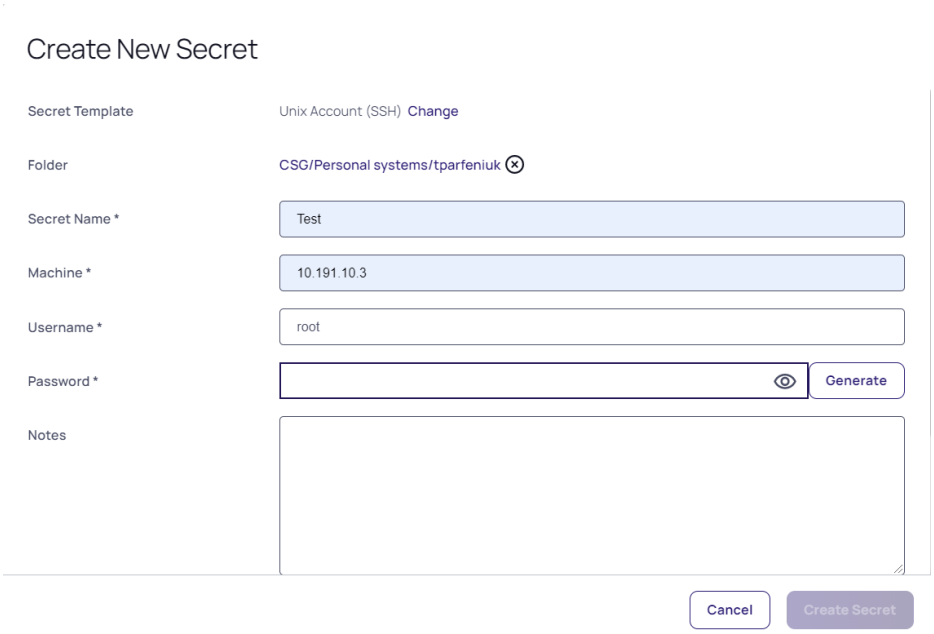

Рис. 3.6. Заповнення полів для нового секрету

Існує чотири рівні дозволів для обміну секретами з іншим користувачем або групою:

View: Користувач може бачити всі секретні дані, такі як ім'я користувача та пароль, а також метадані, такі як дозволи, аудит, історія та налаштування безпеки.

Edit: користувач може редагувати секретні дані. Також дозволяє користувачам переміщати секрет до іншої теки, якщо не увімкнено параметр Успадковувати дозволи з теки, у цьому випадку користувачеві для переміщення секрету потрібні дозволи власника.

List: Користувач може бачити секрет у списку, наприклад, у списку, отриманому в результаті запуску пошуку, але не може переглядати деталі секрету або редагувати його.

Owner: користувач може змінювати всі метадані секрету.

Після створення секрета, стають доступними наступні дії над цим секретом:

Convert Template: Змінити шаблон, який використовується для зберігання і відображення інформації в цьому секреті.

Copy Secret: створити дублікат секрету, який також можна перейменувати і змінити.

Delete: Видалити секрет.

Edit: редагування параметрів секрету.

Favorite:: Натисніть зірочку на Панелі інструментів або встановіть цей прапорець на сторінці перегляду секретів, щоб позначити секрет як обраний. Після цього він відобразиться у віджеті "Вибрані секрети".

Folder: Папка, в якій зберігається секрет. Секрет успадковує дозволи цієї папки, залежно від налаштувань Дозволів секретів за замовчуванням у параметрах конфігурації сервера секретів.

Share: Налаштуйте параметри спільного доступу або дозволи для секрету.

View Audit: Перегляд журналу аудиту секрету, щоб побачити, які користувачі мали доступ до секрету і які дії вони виконували [11].

Закінчення терміну дії секрету - це основна функція Secret Server. Будь-який шаблон можна налаштувати на закінчення терміну дії через певний проміжок часу. Щоб термін дії секрету закінчився, потрібно вибрати текстове поле як ціль для закінчення терміну дії. Наприклад, шаблон секрету для облікових записів Active Directory може вимагати зміну текстового поля пароля кожні 90 днів. Якщо пароль залишається незмінним протягом зазначеного періоду часу, термін дії секрету закінчився, і він з'являється на панелі Expired Secrets на віджеті дашборду Expired Secrets на інформаційній панелі або на головній сторінці.

3.5 Запит доступу до секрету

Функція запиту на доступ дозволяє вимагати схвалення власника секрету перед тим як інший співробітник отримає доступ до нього. Є ключові моменти запиту доступу на консолі Secret Server:

- Створюючи модель робочого процесу, користувач повинен запросити доступ у групи або груп схвалення.

- Усім членам груп затвердження буде надіслано електронного листа з повідомленням про запит.

- Запит може бути схвалений або відхилений будь-яким членом групи затвердження. Затвердження можна встановити за допомогою параметра Require Approval Type, щоб контролювати, хто потребує затвердження.

- Доступ надається на певний період часу.

- Якщо увімкнено параметр Owners and Approvers also Require Approval, то навіть власники або члени групи затвердження повинні запитувати доступ.

- Запитувачі не можуть затверджувати власні запити [11].

Щоб розпочати процес запиту на доступ до секрету, користувач повинен просто спробувати переглянути секрет. Після цього користувач буде перенаправлений на сторінку запиту. Там користувач може пояснити причину запиту, а потім натиснути кнопку **Request Access**, щоб надіслати запит.

Після того, як запит на доступ до секрету було зроблено, затверджувачі отримують електронний лист.

Електронний лист містить одне посилання на сторінку затвердження запиту на доступ до секрету в Secret Server, а також п'ять додаткових посилань для схвалення або відхилення запиту, якщо увімкнено параметр **Allow Approval for Access from Email**.

Затверджувач може або натиснути на одне з посилань, що містяться в електронному листі, або перейти до Notification Center у меню користувача в Secret Server.

3.6 Налаштування політик до секретів в межах PAM

Політика секретів - це набір налаштувань безпеки і віддаленої зміни паролів, які зазвичай застосовуються до секретів на вкладках Безпека або Віддалена зміна паролів. Перевага використання політик полягає не тільки в тому, що налаштування можна застосовувати до секретів масово (тобто за папками), але й у тому, що ці налаштування можна також застосовувати, не даючи користувачам змінювати їх.

Політики секретів слід створювати для застосування параметрів до секретів, які є критичними для робочих процесів компанії. Прикладом створення політики є зміна усіх паролів службових облікових записів кожні 60 днів о 2:00. Політика, яка містить дані параметри може бути застосована до папок, які міститимуть усі ваші службові облікові записи. Щоразу, коли до папки додаватимуться нові облікові записи, наприклад, коли їх буде імпортовано за допомогою виявлення, ці налаштування буде автоматично застосовано і введено в дію (рис.3.7).

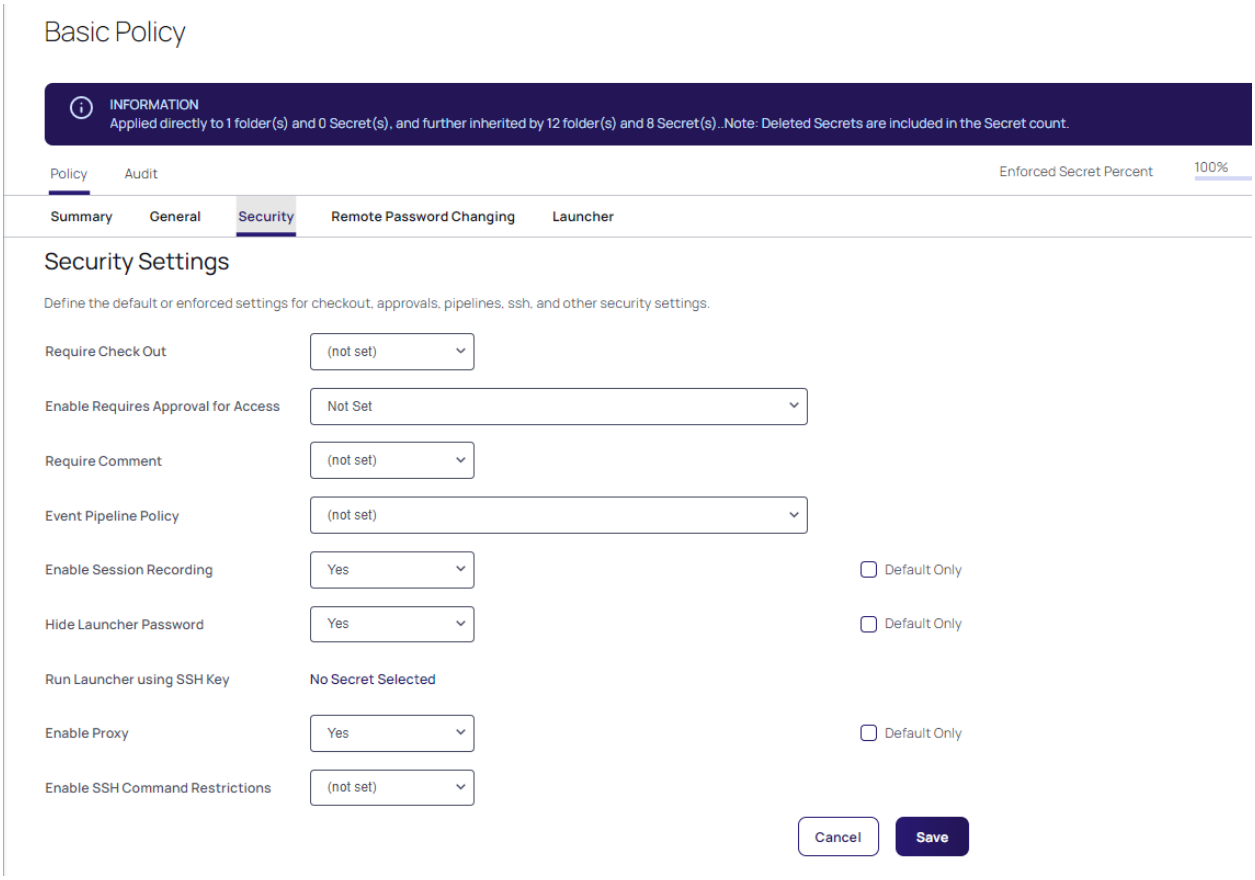

Рис. 3.7. Необхідні для заповлення поля при створенні політики

Політики секретів також можна оновлювати після того, як їх було призначено до папок. Наприклад, якщо парольна політика компанії змінюється і потрібно змінювати паролі службових облікових записів кожні 30 днів, можна оновити політику, і вона буде негайно застосована до всіх секретів, для яких призначено політику [9].

3.7 Надання доступу до корпоративних систем та моніторинг сеансів

Щоб отримати доступ до системи, лаунчер запускає програми на комп'ютерах кінцевих користувачів і автоматично входить в систему, використовуючи облікові дані, що зберігаються на секретному сервері. Загалом, існує три типи лаунчерів: RDP, SSH і користувацький. Це забезпечує зручний спосіб відкриття RDP- і PuTTY-з'єднань, але також позбавляє користувачів необхідності знати свої паролі - користувач може отримати доступ до потрібного комп'ютера, але йому не потрібно переглядати або копіювати пароль з Secret Server. Веб-завантажувач автоматично реєструється на веб-сайтах за допомогою браузера клієнта.

Protocol Handler - це програма на комп'ютері кінцевого користувача. Вона забезпечує зв'язок між сервером і клієнтською машиною. Вона також надає файли, необхідні для запуску. Коли користувач Secret Server запускає програму запуску:

– Protocol Handler завантажує клієнтську програму;

– Protocol Handler зв'язується з сервером за допомогою HTTP або HTTPS протоколу, щоб переконатися, що він має останню версію. Якщо ні, він починає процес оновлення.

– Protocol Handler завантажує цільовий тип програми запуску і починає процес безпечного входу користувача в систему. Окрім транспортного захисту HTTP та HTTPS, облікові дані безпечно передаються з секретного сервера за допомогою підписаних повідомлень, зашифрованих AES-256.

Для критично важливих систем і привілейованих облікових записів іноді недостатньо просто мати аудиторський журнал, який показує, коли хтось переглядав обліковий запис (рис.3.8).

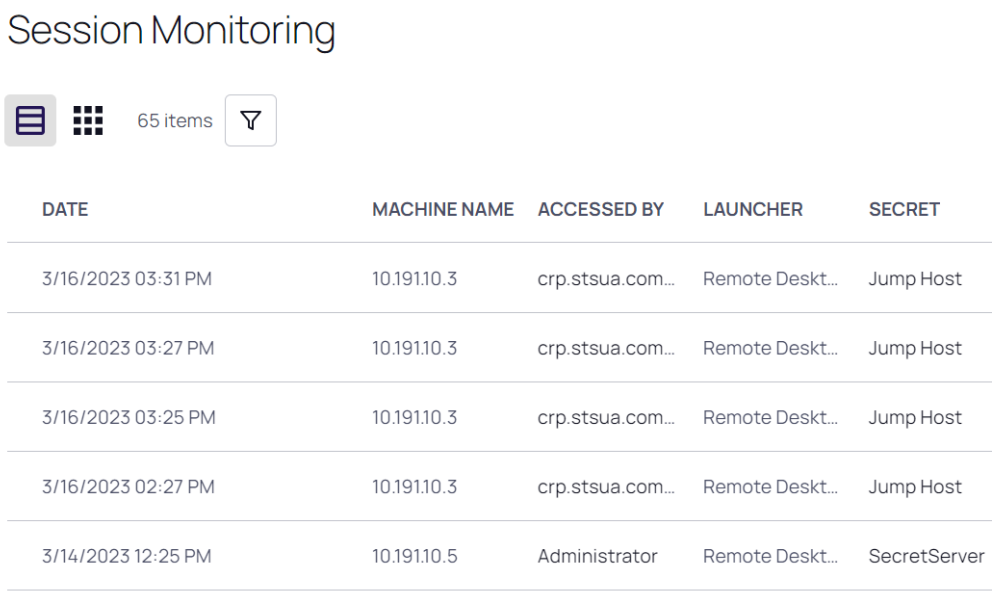

Рис. 3.8. Перегляд записаних сесій у консолі Secret Server

У аудитора може виникнути потреба переглянути, що було зроблено з обліковим записом під час віддаленого сеансу. Для таких критично важливих секретів рекомендується увімкнути запис сеансів для секрета. Коли запис сеансів увімкнено, всі запущені сеанси можуть бути записані для подальшого перегляду аудитором або менеджером, якщо їм потрібно дослідити дії, виконані під час віддаленого сеансу (рис.3.9).

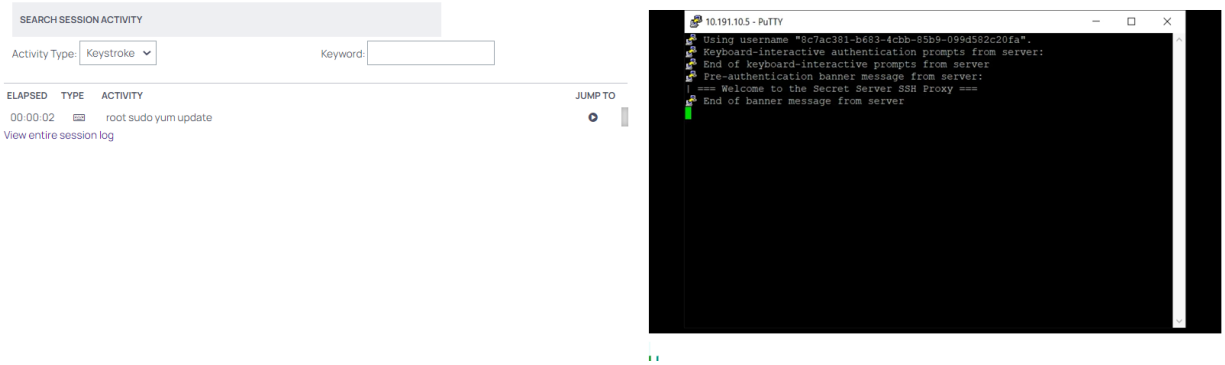

Рис. 3.9. Моніторинг записаної SSH сесії

Відділи можуть визначати це самостійно визначати свої критичні системи, тому залучення їх до узгодження налаштувань моніторингу може бути корисним.

Деякі з цих систем можуть бути чітко відібрані на основі ризиків, вимог державних та міжнародних стандартів або за рекомендацією аудиторської групи.

Одна з найважливіших речей - не вважати всі акаунти чи секрети критично важливими, увімкнувши запис сеансу для них усіх. Це може спричинити проблеми з продуктивністю у середовищі - запис сеансів є найбільш інтенсивною функцією Secret Server.

Перш ніж увімкнути запис сеансів, необхідно оцінити ролі користувачів системи, щоб визначити, хто може контролювати сеанси в реальному часі і переглядати записи. Дозволи, які слід шукати: «адміністрування моніторингу сеансів», «перегляд моніторингу сеансів» і «перегляд записів сеансів».

Моніторинг сеансів можна увімкнути на вкладці Secret для окремого секрету (рис. 3.10) або налаштувати за допомогою політик, які одночасно будуть застосовані до кількох секретів.

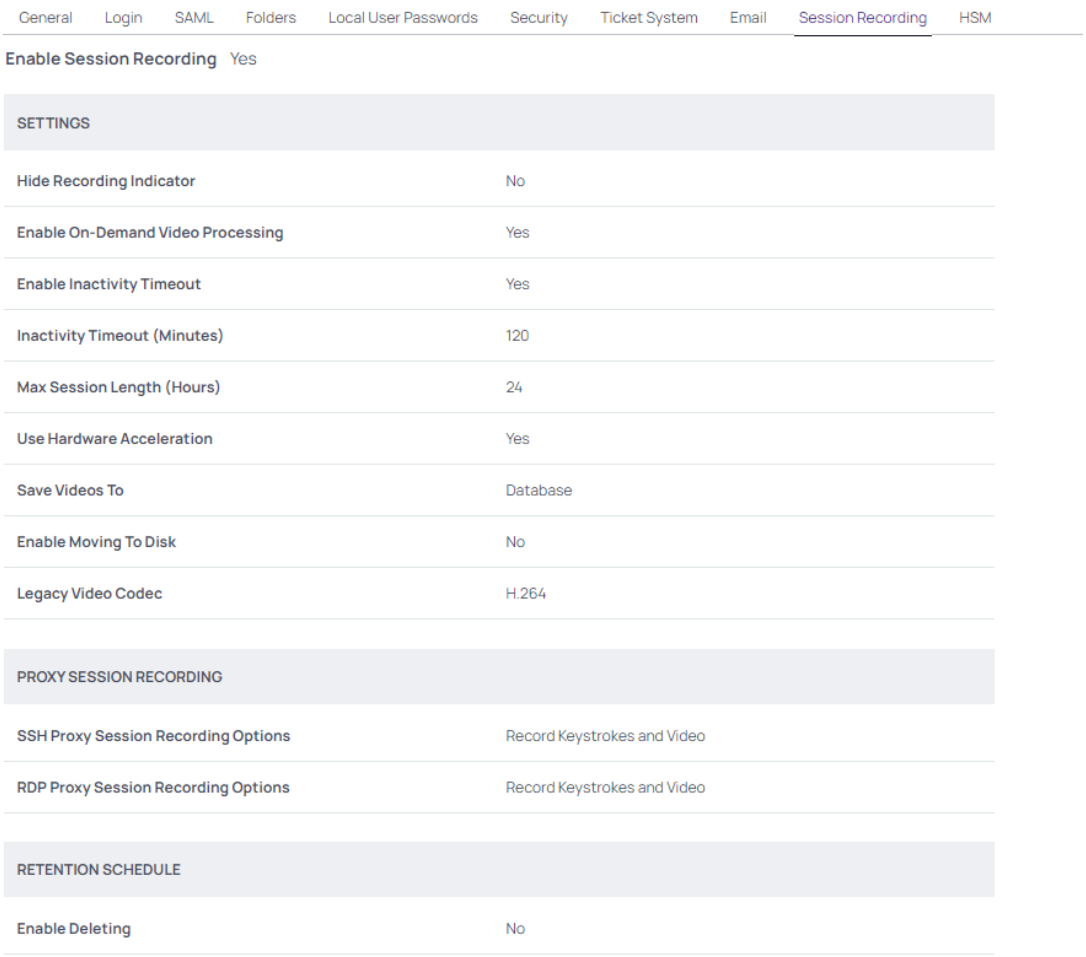

Рис. 3.10. Налаштування запису сеансів

3.8 Налаштування автоматичного виявлення

Виявлення - це процес, під час якого Secret Server сканує середовище для пошуку облікових записів і пов'язаних з ними ресурсів, які називаються залежностями (рис. 3.11). Після того, як облікові записи знайдено, їх можна використовувати для створення нових секретів у Secret Server [11].

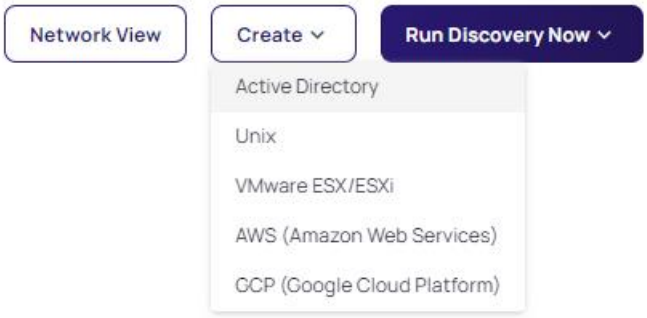

Рис. 3.11. Вибір системи для виявлення облікових записів

Користувачі з правами «адміністрування виявлення» можуть імпортувати облікові записи вручну або створити автоматизований процес для цього (рис. 3.12). Використання виявлення не заважає користувачам створювати власні секрети вручну.

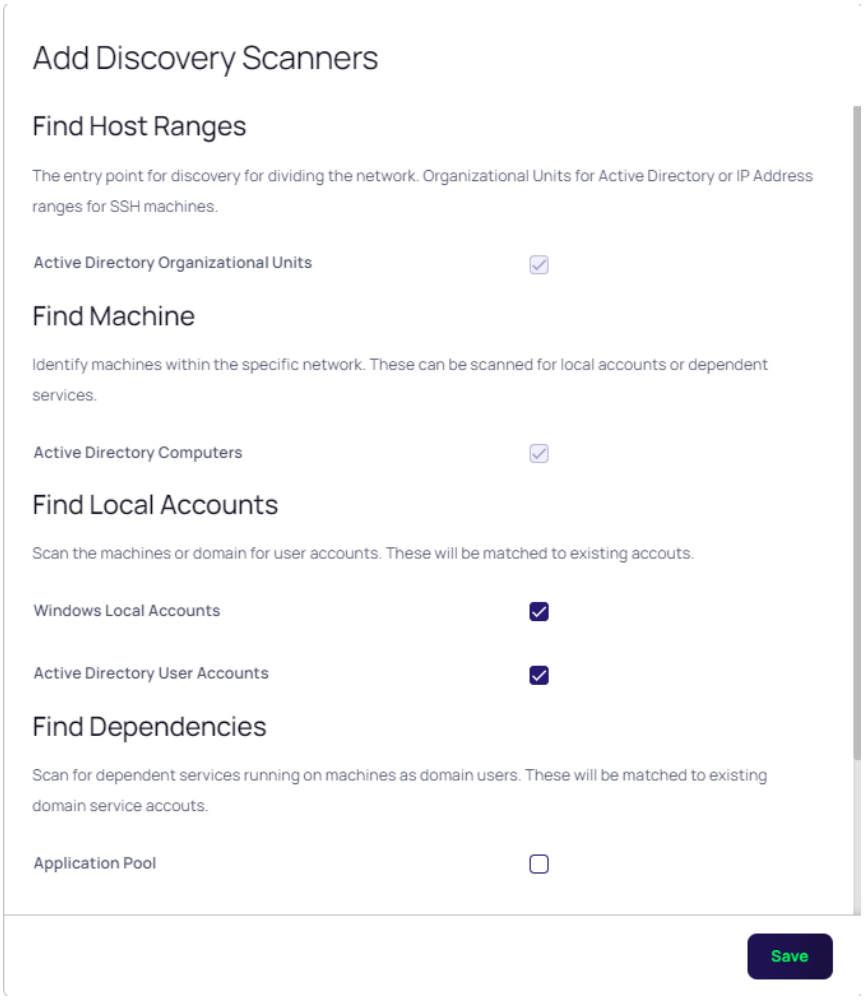

Рис. 3.12. Налаштування процесу виявлення

Серед типових облікових записів, які може знайти виявлення, є локальний адміністратор Windows, домен Windows і Unix. Серед типових залежностей, які може знайти виявлення, - заплановані завдання, запущені від імені користувача домену, пули програм, запущені від імені користувача домену, і служби, запущені від імені користувача домену [11].

Щоб налаштувати Discovery, необхідно перейти в Admin > Discovery та обрати вкладку Create. Звідси потрібно обрати джерело для виявлення та заповнити всі необхідні поля (рис. 3.13).

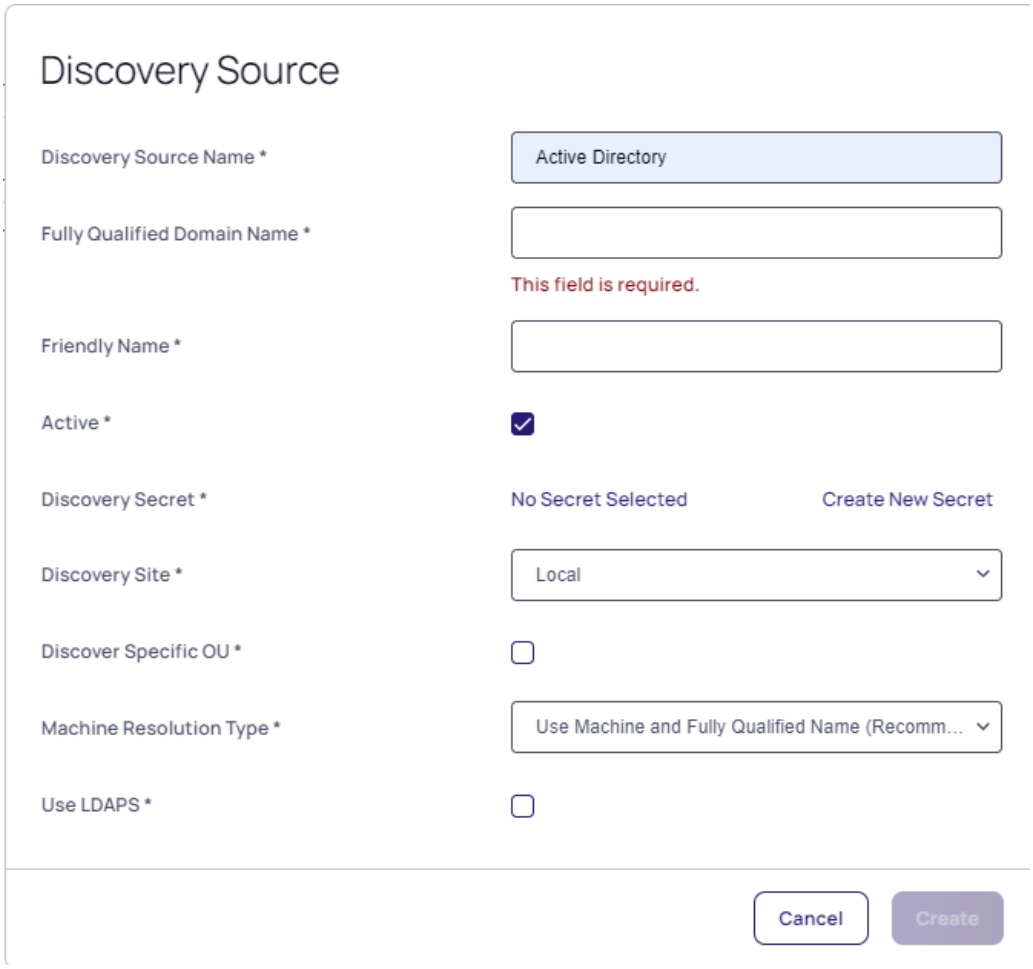

Рис. 3.13. Налаштування Discovery

3.9 Налаштування ієрархії папок

Папки дозволяють створювати контейнери з секретами відповідно до потреб. Вони допомагають упорядкувати клієнтів, комп'ютери, регіони та філії тощо. Папки можуть бути вкладені в інші папки, щоб створити підкатегорії для кожного набору класифікацій. До цих папок і підкатегорій можна призначати секрети. Це дозволяє налаштовувати дозволи на рівні папок, і всі секрети в них можуть успадковувати дозволи папки.

Налаштування дозволів на рівні папки гарантує, що майбутні секрети, розміщені у цій папці, матимуть такі самі дозволи, що спрощує керування для користувачів і груп [9].

Для того, щоб створити нову папку необхідно натиснути плюс в правому куті верхньої панелі Secret Server та обрати **New Folder** (рис. 3.14).

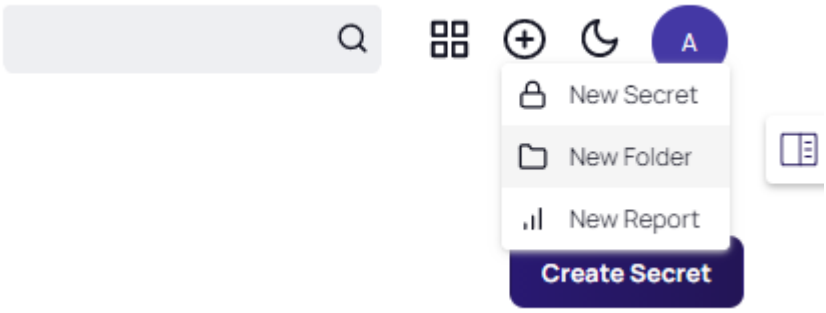

Рис. 3.14. Додавання нової папки

До папок можна застосувати одні з наведених нижче дозволів до користувачів або груп у таблиці **Folder Permissions**:

View: Дозволяє користувачеві бачити папку і її наповнення.

Edit: Дозволяє користувачеві створювати нові папки у цій папці, що примусово встановлює для неї дозвіл «Inherit Permissions from Parent», переміщувати і додавати секрети до цієї папки.

Add Secret: Дозволяє користувачеві додавати облікові записи до цієї папки. Не надає доступу до доданого облікового запису.

Owner: Дозволяє користувачеві створювати нові папки у цій папці без примусового наслідування прав, переміщувати папку, видаляти, перейменовувати, а також змінювати дозволи.

У Secret Server є можливість мати особисту папку. Особисла папка - це папка, доступ до якої має один користувач. Жоден користувач не може змінити права доступу до цих папок. Користувачі можуть додавати підпапки до своїх особистих папок, щоб безпечно зберігати робочі облікові записи або дані, до яких іншим користувачам не потрібен доступ.

3.10 Налаштування робочих процесів

Secret Server підтримує створення access-request workflow, які можна розділити на дві групи:

1. **Multi-Level Workflow**. Початкові запити на доступ є однорівневими або одноступеневими - кожен, хто затверджує запит, затверджує його - жодних інших дій не вимагається. Workflows допускають до 15 етапів затвердження, де схвалення на етапі 1 переносить запит на етап 2, схвалення на етапі 2 переносить його на етап 3 і так далі. Відмова на будь-якому кроці відхиляє запит.
2. **Multiple Approvers to Advance**. Дана функція існує для випадку, коли на певному кроці не вистачає одного затверджувача. В такому випадку, затверджувачі можуть голосувати щодо схвалення, для того щоб воно перейшло на наступний крок [11].

За допомогою створення workflow (рис. 3.15) для запиту на доступ можна:

- Вимагати схвалення запиту кількома особами перед наданням доступу до секрету;
- Вимагати кілька етапів робочого процесу, кожен з яких має різних рецензентів і необхідну кількість схвалювачів, за бажанням;
- Вибирати «власників» як групу рецензування.

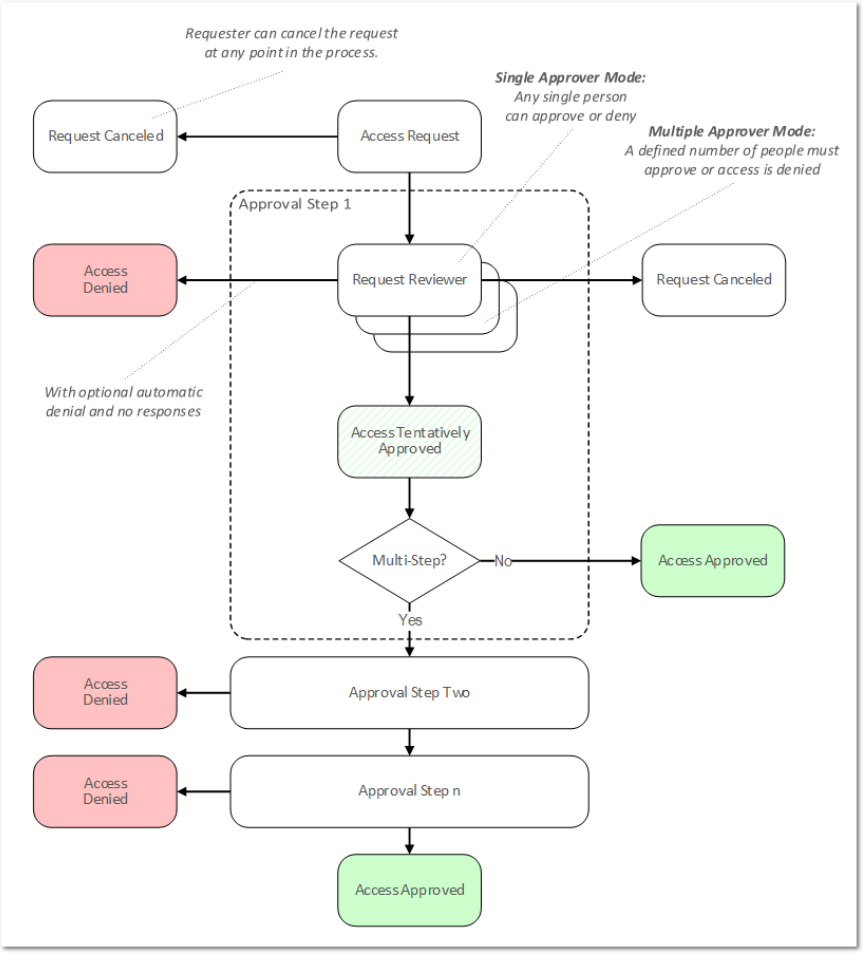

Рис. 3.15. Схема workflow

Для створення нового Workflow, необхыдно перейти у вкладку **Admin** > **Workflows.**

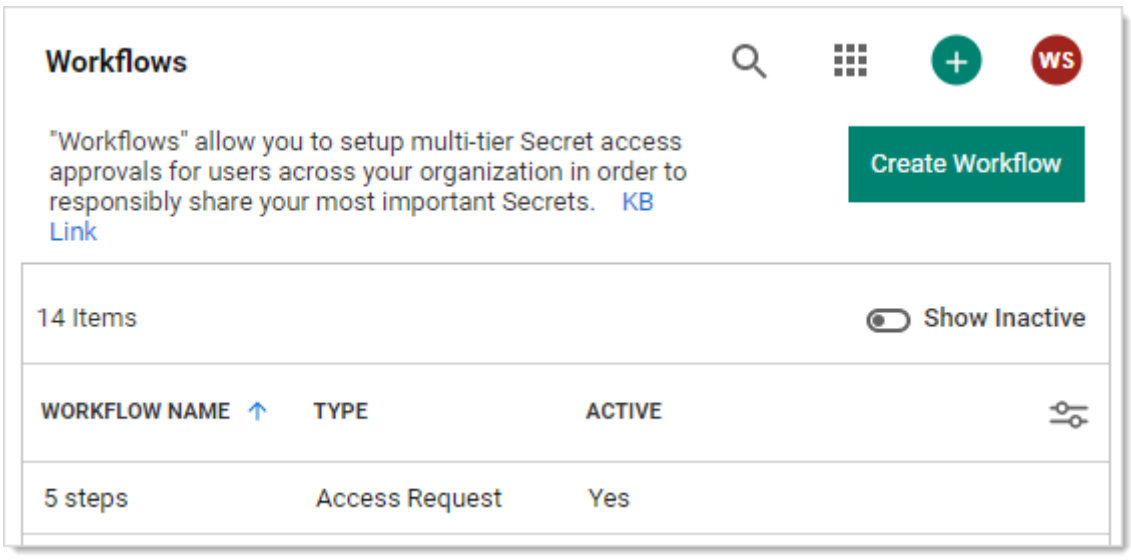

Рис. 3.16. Вкладка Workflows на консолі

Для того, щоб присвоїти створений Workflow для певної політики, щоб зробити його запуск обов'язковим, необхідно перейти у вкладку **Admin > Secret Policy.**

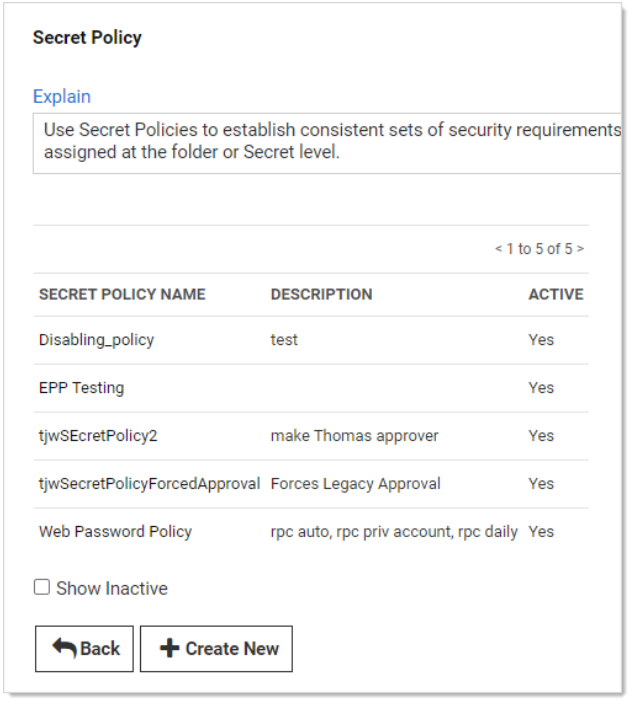

Рис. 3.17. Вкладка Secret Policy на консолі

Далі необхідно настиснути на +Create New. З’виться вікно із налаштуванням нової політики (рис. 3.18).

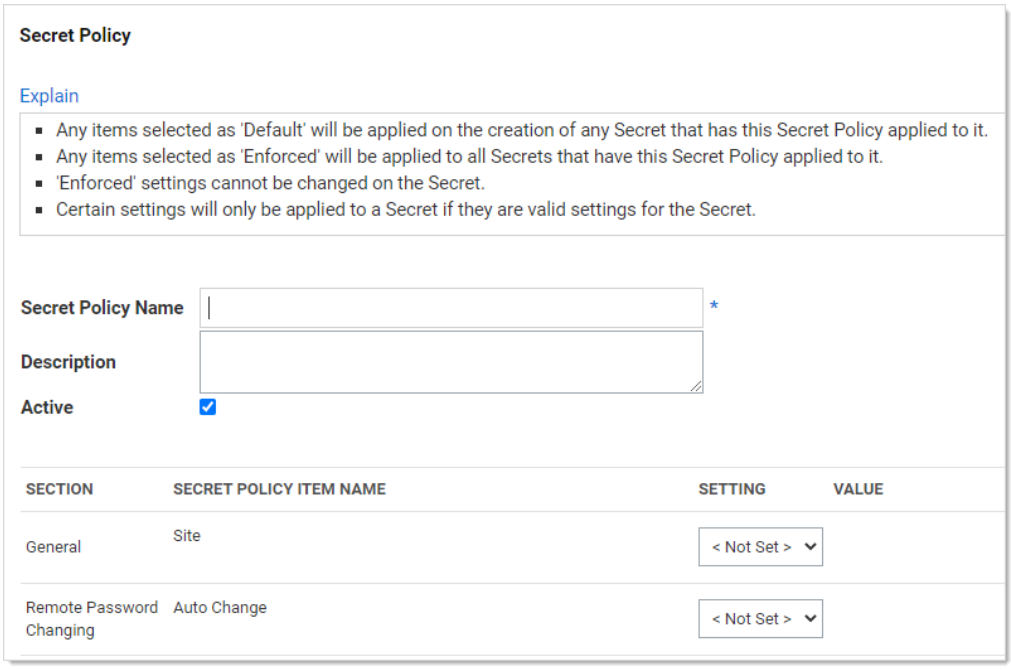

Рис. 3.18. Налаштування нової політики

Далі необхідно звдвти ім'я для даної політики, задати необхідні параметри безпеки. Для того, щоб включити запит на доступ для даної політики, потрібно встановити прапорець біля **Enable Requires Approval for Access.** Після цього необхідно ввести відповідальних, хто буде погоджувати доступ згідно із цією політикою (рис. 3.19).

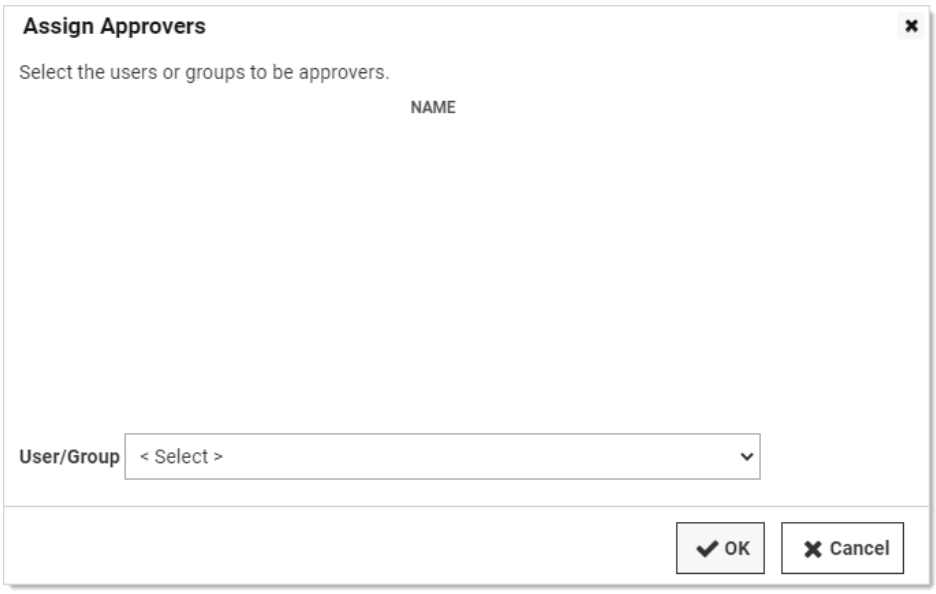

Рис. 3.19. Вибір відповідальних осіб для підтвердження надання доступу

3.11 Керування паролями в межах PAM

Для того, щоб убезпечити доступ користувачів до корпоративних систем, важливо безпечно зберігати дані, яки використовуються для доступу. Для цього сожна використовувати наступні налаштування Secret Server:

– *Приховування паролів на панелі запуску* (рис. 3.20). Часто надання співробітнику доступу до ресурсу через Secret Server не вимагає, щоб він або вона мали доступ до фактичного пароля для облікового запису, який використовується. Якщо програма, яка потрібна користувачеві, може бути запущена за допомогою панелі запуску, користувачеві не потрібно копіювати/вставляти або вводити пароль. Налаштування пароля приховування панелі запуску реалізує наступне: користувачі з доступом до секрету бачитимуть лише зірочки (****) у полі пароля;

поруч з полем не буде значків копіювання в буфер обміну, історії полів або зняття маскування.

Це може бути одним із способів зменшити ризик розкриття паролів привілейованих облікових записів. Приховування паролів запуску можна увімкнути для секретів на вкладці **Security** або за допомогою політики. Також, можна заборонити користувачеві бачити пароль до будь-якого секрету за допомогою панелі запуску, вилучивши з його ролі дозвіл налаштуванням «view launcher password».

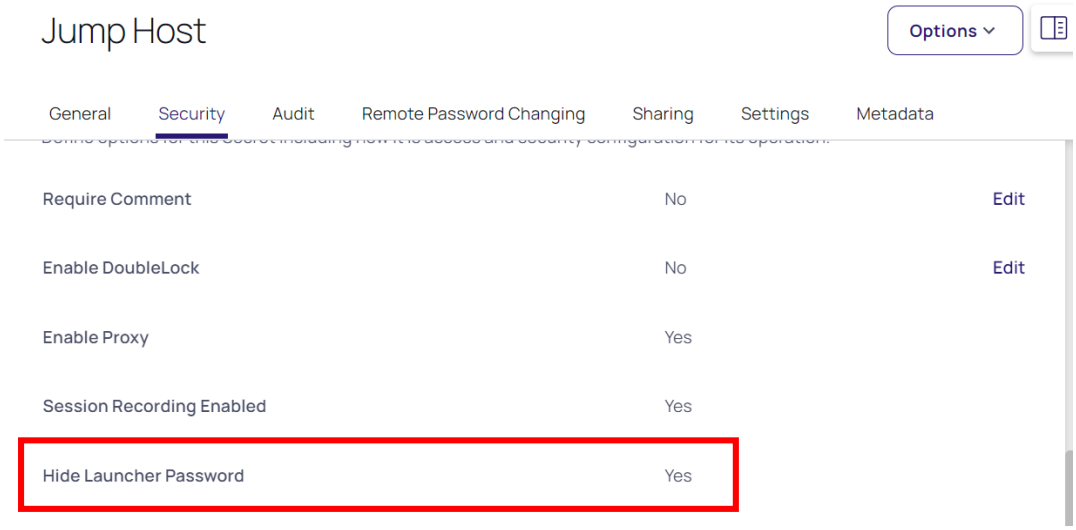

Рис. 3.20. Налаштування увімкнення приховування паролю

– *Вимога ввести коментар* (рис. 3.21). Вимога вводити коментарі під час перегляду секрету може бути чудовим способом переконатися, що користувачі отримують доступ до секрету за необхідності. Коментарі можна переглядати під час проведення аудиту секрету, щоб відстежити, чи був доступ до секрету з початковою метою.

Поширеним прикладом може бути увімкнення функції обов'язкових коментарів для облікового запису адміністратора домену, який зберігається на сервері Secret Server: Користувач може ввести коментар, який вказує на те, що йому або їй потрібно використовувати обліковий запис адміністратора домену, щоб "виконати додавання користувача до групи". У багатьох випадках обліковий запис адміністратора домену не слід використовувати для цієї мети, і часто цю роботу

можна виконати за допомогою менш привілейованого облікового запису в середовищі.

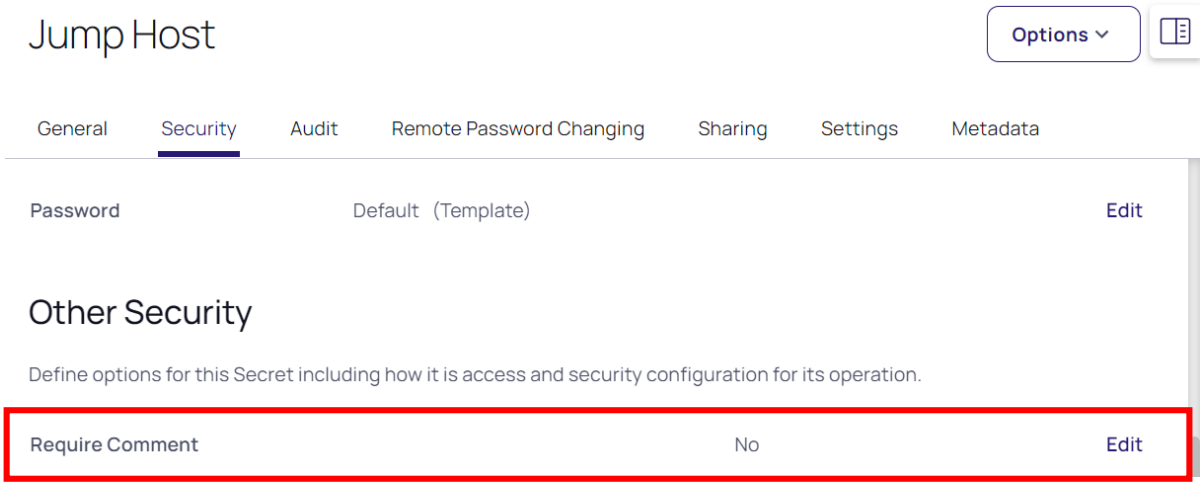

Рис. 3.21. Налаштування увімкнення запиту коментаря

– *Налаштування Check Out.* У випадку, коли користувачі повинні мати прямий доступ до пароля, але є необхідність контролювати, як довго вони можуть користуватися обліковим записом без необхідності щоразу підтверджувати доступ. У цьому випадку приховати пароль для запуску неможливо, але також є проблема щодо того, що користувач знатиме пароль після того, як він його використав. Також часто існує ризик того, що хеш пароля зберігається локально на віддалених пристроях після кожного використання і може бути вразливим до атаки «перехоплення хешу».

Check out може використовуватись наступним чином:

1. Тільки один користувач одночасно має доступ до секрету.
2. Користувач може отримати доступ до секрету лише протягом заздалегідь визначеного інтервалу, наприклад, 30 хвилин.
3. Пароль автоматично буде змінюватися під час входу в обліковий запис користувачем [11].

Облікові записи адміністраторів доменів є чудовим прикладом випадку, коли використання перевірки для зміни пароля при кожному використанні може бути надзвичайно корисним. Це гарантує, що користувачі не будуть копіювати пароль у блокнот або записувати його для подальшого використання, а також зробить

недійсним хеш, який було збережено на віддаленому комп'ютері після сеансу роботи з віддаленим робочим столом.

Перевірка може бути ввімкнена на вкладці Безпека для окремого секрету, але також може бути застосована через політику секретності.

Налаштування Heartbeat. Функція Heartbeat дозволяє секретам автоматично перевіряти введені облікові дані на точність через заданий інтервал часу. Використання серцебиття для секретів гарантує, що ці облікові дані є актуальними, і може попередити адміністраторів про зміну облікових даних за межами Secret Server. Серцебиття допомагає керувати секретами і запобігати їх розбіжності.

На сторінці **Preferences** можна увімкнути параметр Send Email Alerts when Heartbeat Fails, щоб надсилати користувачеві сповіщення електронною поштою, коли серцебиття не відповідає для будь-якого секрету, до якого користувач має доступ для перегляду.

Налаштування Remote Password Changing. Віддалена зміна пароля (RPC) дозволяє секретам автоматично оновлювати відповідні віддалені облікові записи. Це реалізовується шляхом налаштування в секретах автоматичного закінчення терміну дії з подальшою генерацією надійного пароля і віддаленим оновленням пароля, щоб підтримувати синхронізацію облікових записів.

RPC дозволяє Secret Server змінювати паролі відповідно до вимог політики паролів домену. У більшості випадків RPC налаштовується з параметром секрету «auto change», встановленим на **True**. Це призводить до того, що секрет змінює пароль одразу після закінчення терміну його дії. Параметр «auto change schedule» змінює пароль за встановленим розкладом, а не по закінченню терміну його дії. Це дає можливість змінювати паролі, коли мережева активність нижча. Можна змінити пароль, як тільки настане інтервал розкладу або тільки після закінчення терміну дії секрету і настання інтервалу. Важливо вибрати достатньо великий інтервал, щоб завершити всі зміни пароля, інакше будь-які надлишкові зміни доведеться чекати до наступного інтервалу. Якщо Secret Server не змінить віддалений пароль, з'явиться попередження про те, що секрети не синхронізовано.

Щоб налаштувати віддалену зміну пароля необхідно перейти у вкладку **Admin** та далі перейти у **Secret Templates** (рис. 3.22).

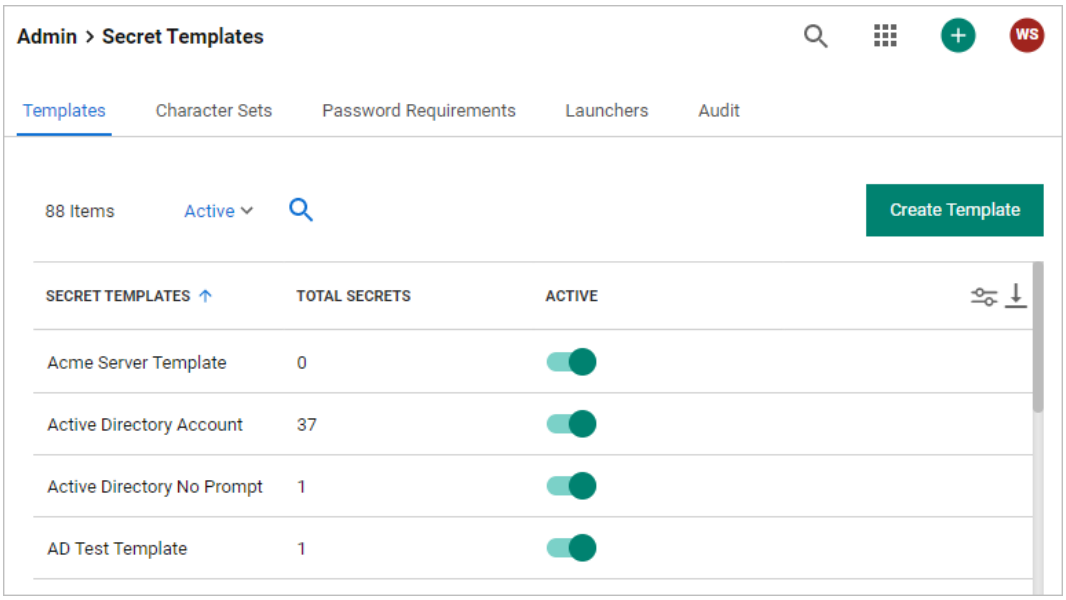

Рис. 3.22. Вкладка Secret Templates на консолі Secret Server

Необхідно обрати назву потрібного шаблону у списку. Відкриється сторінка цього шаблону (рис.3.23):

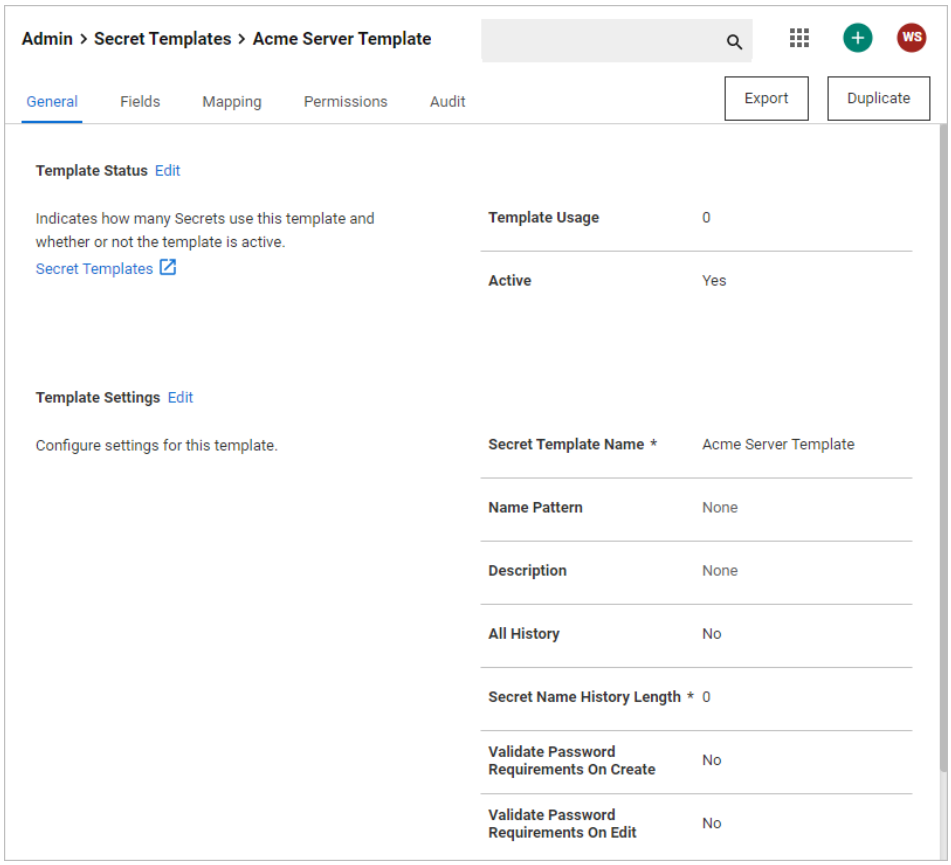

Рис. 3.23. Шаблон Acme Server Template

Необхідно обрати вкладку **Mapping**, обрати Edit та обрати налаштування, що стосується віддаленої зміни пароля (рис.3.24).

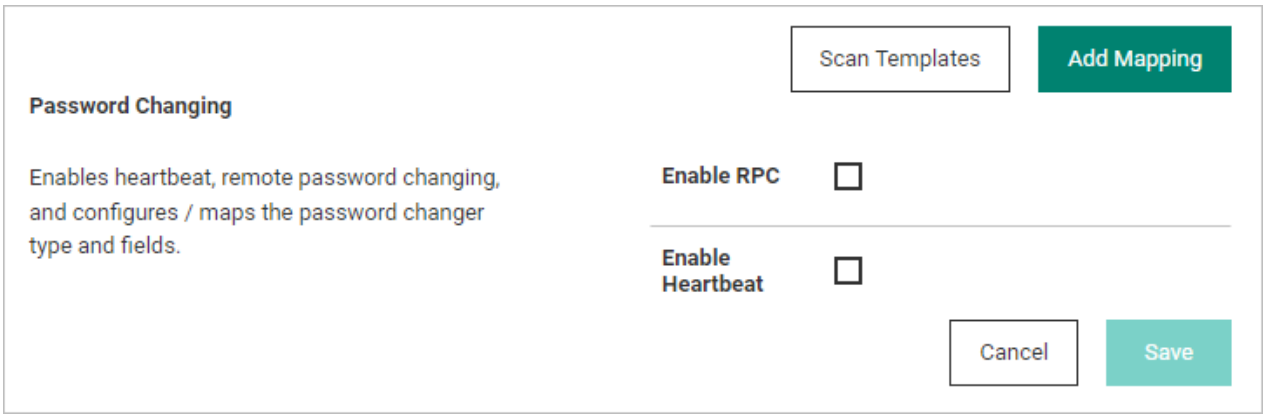

Рис. 3.24. Налаштування віддаленої зміни пароля

Після цього необхідно заповнити необхідні поля, щоб встановити інтервал зміни пароля для даного шаблону (рис.3.21).

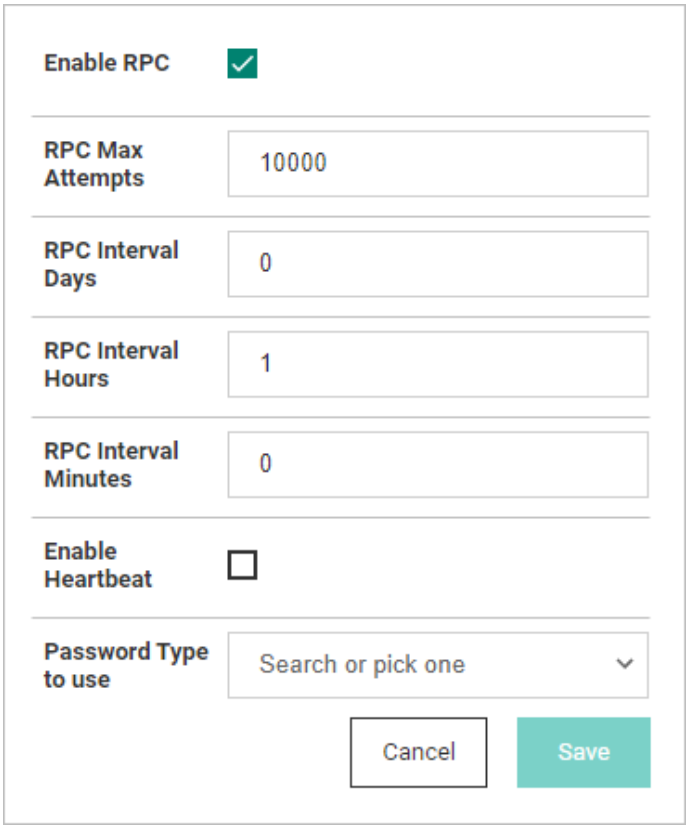

Рис. 3.25. Налаштування інтервалів для зміни пароля

3.12 Налаштування подій всередині Secret Server

Event Pipeline (EP) - це іменована група тригерів, фільтрів і завдань для управління подіями та реакціями на них. Самі Event Pipeline можуть бути згруповані в політики EP.

Event Pipeline може включати наступні компоненти:

Event Pipeline Policy - це іменована група подій, які запускаються одночасно (у послідовному порядку). Як і події, політики конвеєра подій бувають двох типів: секретні та користувацькі. Секретні політики EP націлені на секретні політики або папки і можуть містити лише секретні EP. Користувацькі політики EP націлені на користувачів у групах і можуть містити лише користувацькі EP. Для роботи політики EP повинні мати призначений об'єкт політики EP.

Фільтри EP - це параметри, які обмежують час запуску завдань EP. Усі фільтри мають налаштування і можуть бути додані до EP кілька разів.

Event Pipeline Policy Target є папки секретного сервера, політики секретності або групи користувачів, до яких застосовується політика EP. Для секретних типів EP, секрети всередині папок або секрети під секретними політиками запускають EP в політиці EP. Як об'єкти, папки не є рекурсивними - лише секрети безпосередньо в папці можуть викликати EP. Для типів користувацьких EP лише користувачі у вибраних групах можуть викликати EP.

EP tasks - це дії, які запускаються в EP, якщо виконуються будь-які умови фільтрації. Завдання можуть редагувати секрети, переміщувати секрети, змінювати дозволи, надсилати сповіщення тощо.

Event Subscriptions. Event Subscriptions запускають сповіщення про визначені події в системі. Ці сповіщення надсилаються на поштову скриньку, а звідти можуть бути надіслані назовні електронною поштою або через Slack.

Для налаштування даного функціоналу необхідно перейти до вкладки **Admin > Event Subscriptions** (рис. 3.26).

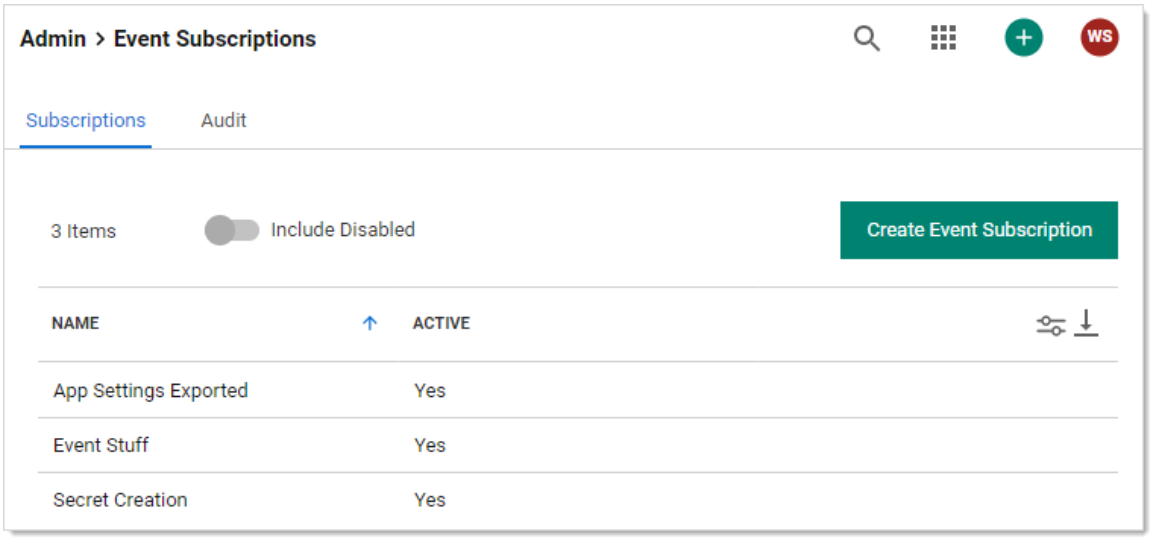

Рис. 3.26. Вкладка Event Subscription

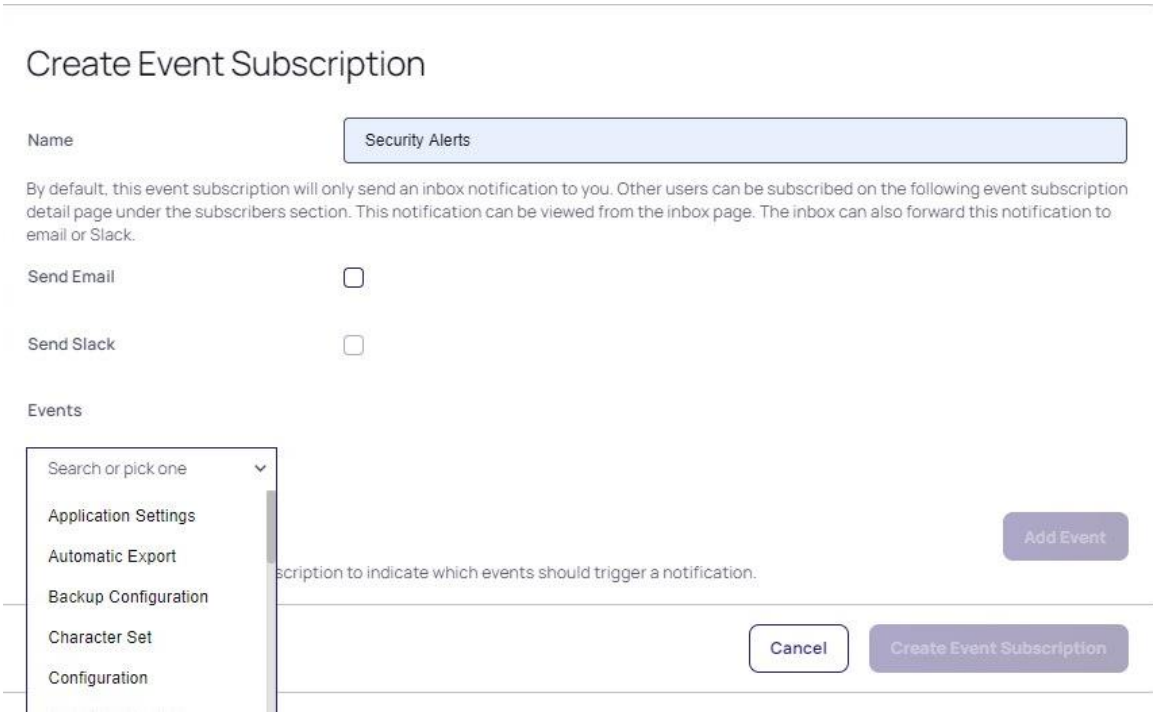

Рис. 3.26. Налаштування Event Subscription

Сторінка **Event Subscriptions** включає в себе:

Event Subscriptions: Назва підписки на подію, чи є вона активною і як довго сповіщення від останньої до закінчення терміну дії залишатимуться у папці **Inbox**.

Події:

Send Email with High Priority: Надсилає імейл для цієї підписки з високим пріоритетом.

Subscribed Events: Список подій, які містяться в цій підписці.

Subscribed Users: Список користувачів і груп секретного сервера, підписаних на цю подію [9].

3.13 Налаштування SSH Proxy

Проксі-сервер Secret Server направляє SSH і RDP сесії та допомагає захистити облікові дані кінцевих точок.

Для того, щоб налаштувати перенаправляння трафіку необхідно перейти до **Admin > Proxying** та дозволити налаштування SSH Proxying та згенерувати новий ключ.

Функція RDP-proxying дозволяє перенаправляти RDP з'єднання, встановлені за допомогою панелі запуску, через Secret Server. Це може бути налаштуване одним із двох способів:

3. Рекомендований спосіб: Програма запуску підключається до нової сесії з тимчасовими обліковими даними, а RDP-проксі з'єднується з віддаленим сервером, використовуючи захищені облікові дані з секрету. Цьому методу надається перевага, оскільки він запобігає потраплянню секретних облікових даних на клієнтську машину. Для цього методу достатньо налаштовувати RDP-проксі.

Спосіб реалізації даного методу:

- Користувач натискає на кнопку запуску RDP в консолі Secret Server.
- Програма запуску виконується на клієнтському комп’ютері.
- Засіб запуску встановлює з'єднання з RDP-проксі, використовуючи облікові дані, згенеровані для даного сеансу.
- Після успішної автентифікації, RDP-проксі сервер шукає облікові дані та ім'я цільового хоста, до якого потрібно з'єднатися.
- RDP-проксі з'єднується з потрібним віддаленим хостом за допомогою тимчасових облікових даних.
- Встановлюється RDP-сесія.

- RDP-трафік пересилається через RDP-проксі, натискання клавіш під час сеансу відстежується, якщо увімкнено запис сеансу.

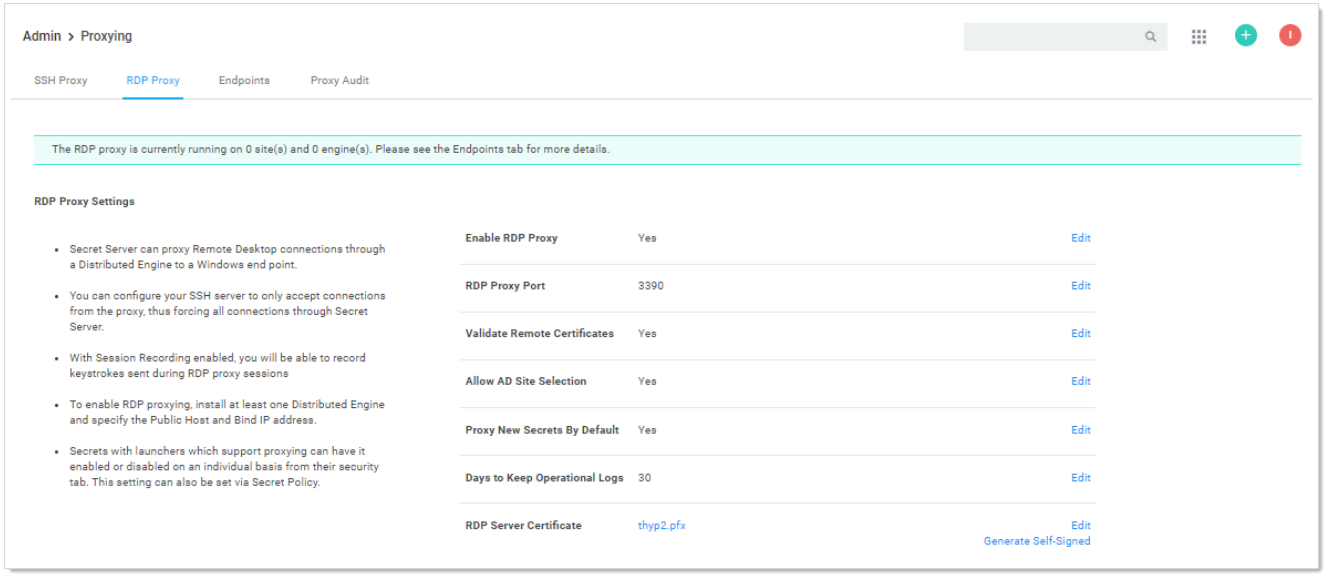

Рис. 3.27. Налаштування SSH Proxy

4. Альтернативний спосіб: Програма запуску використовує SSH-проксі для тунелювання локального RDP-з'єднання до віддаленого сервера. Цей метод не захищає облікові дані від потрапляння на клієнтську машину. Для цього методу ви налаштовується SSH-проксі-сервер і вмикається тунелювання SSH.

Висновки до третього розділу

Розглянуто процес налаштування рішення для організації доступу до корпоративних систем Secret Server. На консолі налаштувано ролі, що відповідають за розмежування доступу до корпоративних систем.

Досліджено моніторинг записаних сесій, що дозволяє контролювати всі дії, виконані користувачами у межах корпоративних систем.

Розроблено рекомендації, щодо поводження із обліковими даними в межах консолі рішення та наведено способи їх захисту.

ВИСНОВКИ

В бакалаврській роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено поняття облікового запису та прівелейованого облікового запису, а також розкрито потенційні ризики, з якими вони можуть стрикнутись компанії. Саме це підтверджує актуальність даного дослідження.

2. Проаналізовано рішення класу PAM, їх функціоналу. Досліджено модулі, з яких можуть складатись рішення та описанно можливості цих модулів на прикладі двох рішеня: Thycotic Secret Server та OneIdentity Safeguard.

3. Досліджено необхідні етапи, які організація повинна пройти перед вибором рішення PAM та перед впровадженням його у свою компанію.

4. Розгорнуто рішення Thycotic Secret Server у тестовому середовищі, для детальнішого ознайомлення із його функціональними можливостями.

5. Розроблено рекомендації щодо впровадження та налаштування рішення Thycotic Secret Server з точки зору організації доступу до корпоративних систем. Дані рекомендації можуть бути використані аналітиками інформаційної безпеки та інженерами відділу інформаційної безпеки.