ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ КОРИСТУВАЧІВ ІС ОРГАНІЗАЦІЇ НА БАЗІ РІШЕНЬ ІВМ»

Виконала студентка 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Нечипуренко К.О.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
"___" _____ 2021 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Нечипуренко Ксенії Олександрівні
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія управління привілейованим доступом користувачів іс організації на базі рішень ІВМ»
керівник магістерської роботи Гайдур Галина Іванівна, д.т.н, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2021 року № 170

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
інформаційна система;
програмні комплекси для управління привілейованим доступом;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення інформаційної безпеки корпоративної інформаційної системи.
2. Аналіз методів та засобів управління привілейованим доступом на базі IBM Security Verify Privilege Vault.

3. Розроблення варіанта технології управління привілейованим доступом на базі IBM Security Verify Privilege Vault.

5. Перелік графічного матеріалу

1.
2.
3.
4.
5.
6.
7.
8.
9.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Вивчення актуальності проблеми управління привілейованим доступом сучасного підприємства	27.09.2021 р.	
2.	Аналіз науково-технічної літератури з питань теми магістерської роботи.	12.10.2020 р.	
3.	Аналіз методів та засобів управління привілейованим доступом.	23.10.2020 р.	
4.	Розроблення системи управління привілейованим доступом.	14.11.2020 р.	
5.	Розроблення рекомендацій щодо застосування технології управління привілейованим доступом.	02.12.2020 р.	
6.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студентка Нечипуренко К.О.
(підпис) (прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студентки Нечипуренко Ксенії Олександрівни

на тему: «Технологія управління привілейованим доступом користувачів іс організації на базі рішень IBM»

Актуальність: У кожній організації є ключові співробітники, які мають доступ до критичних бізнес-додатків. Облікові дані для цих програм мають бути суворо захищені. Часто в цих програмах зберігається життєво важлива, конфіденційна інформація, і несанкціонований доступ може коштувати бізнесу цілих грошей.

Сфера привілейованого доступу може змінюватися від одного бізнесу до іншого. Наприклад, компанія, що займається медичною та фармацевтичною промисловістю, може потребувати привілейованого доступу до програм і програмного забезпечення, яке використовується командою досліджень і розробок, що містить конфіденційні дані.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми управління привілейованим доступом та визначено мету та завдання для досягнення поставлених цілей.
2. Було досліджено методи та засоби управління привілейованим доступом на базі рішення IBM.
3. Запропоновано варіант технології системи управління привілейованим доступом на базі рішення IBM.
4. Текст викладено грамотно і послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести аналіз умов функціонування системи управління привілейованим доступом корпоративних інформаційних систем на прикладі конкретного підприємства.
2. Запропонований варіант управління привілейованим доступом на базі рішення IBM бажано було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **добре**, а студентка **Нечипуренко К.О.** – присвоєння кваліфікації: магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студентка Нечипуренко К.О.. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)
освітньо-професійної програми Інформаційна та кібернетична безпека
на тему: «Технологія управління привілейованим доступом користувачів іс організації на базі рішень ІВМ».
Магістерська робота і рецензія додаються.
Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Нечипуренко К.О. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року до 2022 року повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Журенко О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка ***Нечипуренко К.О.*** обрала тему роботи, метою якої було дослідити зміст технології управління привілейованим доступом сучасного підприємства на базі рішення ІВМ та розробити варіант алгоритму управління привілейованим доступом. Перелік використаних джерел свідчить про вміння дипломником розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Нечипуренко К.О. показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Керівник магістерської роботи _____ Гайдур Г.І..
(підпис) (прізвище та ініціали)

"___"_____2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студентка Нечипуренко К.О.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 68 сторінок, 22 рисунки, 2 таблиці, 13 джерел.

Об'єкт дослідження: процес забезпечення управління привілейованим доступом сучасного підприємства.

Предмет дослідження: технологія управління привілейованим доступом підприємства.

Мета роботи: розробити технологію для забезпечення привілейованим доступом.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів управління привілейованим доступом.

В роботі проведено аналіз проблеми забезпечення управління привілейованим доступом сучасного підприємства та визначені мета та завдання щодо підвищення можливостей управління привілейованим доступом.

Були визначені можливості програмного комплексу IBM Security Verify Privilege Vault та його основні архітектурні особливості щодо реалізації управління привілейованим доступом. Надані інструкції по базовій конфігурації для корпоративної інформаційної системи.

Проаналізовано можливості програмного комплексу IBM Security Verify Privilege Vault щодо виконання процесу управління привілейованим доступом у сучасному підприємстві.

Галузь використання – кібербезпека.

РАМ, КІБЕРБЕЗПЕКА, ПРИВІЛЕЙОВАНИЙ ДОСТУП, УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ, ЧУТЛИВІ ДАНІ, IBM SECURITY VERIFY PRIVILEGE VAULT.

ABSTRACT

Master’s thesis: 68 pages, 22 figures, 2 tables, 13 sources.

Object of research: the process of ensuring the management of privileged access of a modern enterprise.

Subject of research: technology of management of privileged access of the enterprise.

Purpose: to develop technology to provide privileged access.

Research methods: elaboration of literature on this topic, analysis of operational documentation, international standards and their comparison, practical use of privileged access management tools.

The paper analyzes the problem of providing privileged access management of a modern enterprise and identifies goals and objectives to increase the ability to manage privileged access.

The capabilities of the IBM Security Verify Privilege Vault software package and its main architectural features for the implementation of privileged access management were identified. Basic configuration instructions for the corporate information system are provided.

The possibilities of the IBM Security Verify Privilege Vault software package for the implementation of the privileged access management process in a modern enterprise are analyzed.

Field of use – cybersecurity of an organization's information system.

PAM, CYBER SECURITY, PRIVILEGED ACCESS, PRIVILEGED ACCESS MANAGEMENT, METHODS AND MEANS OF PRIVILEGED ACCESS MANAGEMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІТ – інформаційні технології

PAM – Privilege Access Management

ІС – Інформаційна Система

КІС – Корпоративна Інформаційна Система

HTTP – Hypertext Transfer Protocol

ОТ – Операційні технології

IoT – Internet of things

SE – Social engineering

URL – Uniform Resource Locator

ВСТУП

У кожній організації є ключові співробітники, які мають доступ до критичних бізнес-додатків. Облікові дані для цих програм мають бути суворо захищені. Часто в цих програмах зберігається життєво важлива, конфіденційна інформація, і несанкціонований доступ може коштувати бізнесу цілих грошей.

Сфера привілейованого доступу може змінюватися від одного бізнесу до іншого. Наприклад, компанія, що займається медичною та фармацевтичною промисловістю, може потребувати привілейованого доступу до програм і програмного забезпечення, яке використовується командою досліджень і розробок, що містить конфіденційні дані.

Аналогічно, IT-адміністратор, який створює, відстежує та видаляє облікові записи співробітників, потребує привілейованого доступу.

Тому кожен, чий доступ до програми, програмного забезпечення або інструменту, що містить інформацію, яка є надзвичайно важливою для компанії, має підпадати під «привілейований доступ».

Об’єктом дослідження є процес забезпечення управління привілейованим доступом на сучасному підприємстві.

Предметом дослідження є технологія управління привілейованим доступом на сучасному підприємстві.

Метою роботи є розробка системи для забезпечення управління привілейованим доступом.

Для досягнення цієї мети були поставлені такі наукові завдання:

1) дослідити зміст управління привілейованим доступом;
2) проаналізувати існуючі методи та засоби управління привілейованим доступом;
3) дослідити можливості застосування програмного комплексу IBM Security Verify Privilege Vault з метою забезпечення управління управління привілейованим доступом на сучасному підприємстві.

Практичне значення одержаних результатів полягає у розробці рекомендацій та технології щодо управління привілейованим доступом на основі програмного комплексу IBM Security Verify Privilege Vault.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи

Корпоративна інформаційна система – це управлінські ідеологія, що поєднує бізнес-стратегію підприємства (з 4 будованою для її реалізації структурою) і передові інформаційні технології. Прийнято вважати, що головну увагу при цьому приділяють відпрацьованій структурі керування, що складає функціональну частину підприємства, а автоматизація виконує другорядну, інструментальну роль [1]. Корпоративна 1С є інформаційно-керуючою системою, що включає бізнес архітектуру підприємства, його персонал, IT-архітектуру та є діючою частиною кіберкорпорації. Рис. 1.1 є ілюстрацією тришарової архітектури схеми сучасного підприємства – кіберкорпорації, де 1С – частина підприємстві яка здійснює бізнес, або організаційно виробничу діяльність. «Корпоративність» у терміні КІС означає відповідність системи вимогам великої фірми, що має складну структуру, великі кількість взаємодіючих компонентів з ієрархічністю підпорядкування цілей їх діяльності загальній меті усієї системи. Інформаційні системи окремих підрозділів фірми (фінансових, економічних, маркетингових та ін.) не можуть претендувати на корпоративність. Тільки повнофункціональна система може дійсно бути охарактеризована як КІС.

Рис. 1.1. Тришарова схема сучасного підприємства – кіберкорпорації

Суть системного підходу до проектування економічних 1С полягає в комплексному вивченні об'єкта керування як єдиного цілого на основі аналізу і синтезу. Аналіз припускає виділення ознак структуризації і декомпозиції системи. Економічна система є складною багатофункціональною. Тому існує безліч способів її декомпозиції.

Традиційно економічну інформаційну систему розглядають як сукупність двох компонентів або підсистем – функціональної і забезпечувальної. Функціональна частина є моделлю системи керування об'єктом і, як будь-яка модель, вимагає чіткого математичного обґрунтування й опису [1]. Забезпечувальна частина припускав такі види забезпечення, як математичне, технічне, програмне, інформаційне, лінгвістичне, організаційне, правове, ергономічне. Синтез полягає в інтеграції успадкованих систем з новітніми розробками 1С, інтеграції модулів 1С, реалізованих у гетерогенному обчислювальному середовищі, вимагає наявності розвинутих засобів інтероперабельності поєднуваних компонентів. У загальному випадку інтероперабельність – властивість, яка припускає здатність різних або подібних середовищ, систем чи функціональних елементів взаємодіяти один з одним, що повинно забезпечуватися їх безперешкодним інтерфейсом, заснованим на відкритості їх стосовно одне одного [3].

Інтерфейс у широкому розумінні – це сукупність уніфікованих засобів організації взаємодії різних систем або функціональних елементів однієї системи. Інтероперабельність зумовлює правила композиції окремих компонентів у цілісну систему і спирається на стандарти. Стандарти застосовуються скрізь як при розробці функціональної, так і забезпечувальної компонент 1С; у забезпечувальній частині - від комунікацій до керування базами даних і додатками. Рис. 2.2 ілюструє зв'язок між розподілом компонент 1С, їх неоднорідністю і стандартами [2].

Рис.1.2. Взаємозв'язок між розподілом компонент ІС їх неоднорідністю і стандартами

Обов'язковим організуючим елементом розробки корпоративних систем є стандарти. Кожна корпорація в процесі розробки та експлуатації 1С керується корпоративними стандартами (КС), які базуються на галузевих, національних та міжнародних стандартах [4; 2]. Стандарти відображують рівень розвитку культури керування, рівень технологічного розвитку, рівень розвитку законодавства. Використання стандартів є однією з головних передумов для створення відкритих систем. Вихід на міжнародні ринки вимагає орієнтації на міжнародні стандарти. Це стосується не тільки стандартів на продукцію та по слуги. Участь у міжнародних проектах вимагає від фірм впровадження міжнародних стандартів.

Орієнтація на міжнародні інвестиції вимагає постановки фінансового обліку за міжнародними стандартами. Роблячи національні або міжнародні стандарти своїми КС організація набуває більшої гнучкості та мобільності. Вона починає використовувати весь досвід керування, сконцентрований у цих стандартах, і одержує серйозні конкурентні переваги. У цьому випадку й автоматизація одержує

надійну точку опори. На міжнародних ринках конкуренція товарів і технологій уже перетворилася на боротьбу стандартів. Особливо яскраво це демонструють ринки апаратного і програмного забезпечення. Будь-якій організації варто усвідомлювати, що приймаючи в якості корпоративного стандарт однієї зі сторін-конкурентів, вона робить серйозний стратегічний вибір [6].

Можна умовно виділити три види управлінської діяльності, які регулюються управлінськими корпоративними стандартами (УКСт), це:

- планування;
- облік;
- прийняття рішень.

Кожний із зазначених видів діяльності реалізується в конкретній предметній сфері корпоративного управління, і кожна така предметна сфера може мати свою галузеву специфіку. Нині немає стандартів, що визначають функціонування KIQ. Однак широко розповсюджені методології MRP II {Manufacturing Resource Planning) і ERP {Enterprise Resource Planning) американської дослідницької компанії Gartner Group є на сьогоднішній день основою для розробок у цій області. Практично всі сучасні програмні продукти масштабу підприємства засновані на стандарті MRPII і більш новій методології ERP На жаль, підходи до цих питань у країнах СНД обмежуються стандартами на автоматизовані системи керування (АСУ), що фактично є технологічними прийомами і методичними вказівками, які дозволяють дотримуватись визначених правил при створенні систем автоматизації різних видів – систем автоматизованого проектування (САПР), автоматизованих систем керування технологічними процесами (АСУТП) та ін.[6].

1.1.1. Стандарт методів управління виробництвом і дистрибуції МИР II

Стандарт методів управління виробництвом і дистрибуції TiARPII розроблений американським суспільством для контролю за виробництвом і запасами (American Production and Inventory Control Society). На думку творців,

стандарт являє собою набір перевірених на практиці принципів, моделей і процедур керування і контролю, спрямованих на підвищення економічної ефективності діяльності підприємства [5]. Історія MRP II починається з 60-х років. Згодом стандарт реформувався й охоплював усе більше виробничих і невиробничих операцій. Так, у 60-70-х роках регламентувалася лише сфера планування потреб у матеріалах, ґрунтуючись на даних про запаси (Material Requierment Planning). У 70-80-х роках розглядалося вже планування потреб у матеріалах за замкнутим циклом (Cloosed Loop Material Requirment Planning).

На початку 90-х років була охоплена сфера прогнозування, планування і контролю за виробництвом на основі даних, отриманих від постачальників і споживачів. До початку XXI сторіччя стандарт MRPII описує планування потреб у розподілі ресурсів на рівні підприємства (Enterprise Resourse Planning та Distributed Requirements Planning).

Структура MRP II точно відповідає функціональним групам виробничої системи, таким як [6]:

1. Планування продажів і виробництва - Sales and Operation Planning.
2. Керування попитом – Demand Management.
3. Складання плану виробництва – Master Production Scheduling.
4. Планування матеріальних потреб – Material Requirement Planning.
5. Специфікація продуктів – Bill of Materials.
6. Керування складом – Inventory Transaction Subsystem.
7. Планові постачання – Scheduled Receipts Subsystem.
8. Керування на рівні виробничого цеху – Shop Flow Control.
9. Планування виробничих потужностей – Capacity Requirement Planning.
10. Контроль показників на вході і виході:Input/output control.
11. Матеріально-технічне постачання – Purchasing.
12. Планування ресурсів реалізації товарів – Distributioj Resource Planning.
13. Планування і контроль виробничих операцій – TooliiJ Planning and Control.
14. Фінансове планування – Financial Planning.

15. Моделювання – Simulation.

16. Оцінка результатів діяльності – Performance Measuremen.

1.1.2. Організація інформаційних систем у відповідності до стандарту MRPII

Метою побудови інформаційних систем у відповідності зі стандартом MRPII є забезпечення оптимального формування потоків матеріалів (сировини і напівфабрикатів) і готових виробів.

При правильній організації створення і застосування інформаційних систем за стандартом MRPII можуть бути забезпечені такі функції, як [5]:

- інформування керівництва підприємства про результати діяльності всіх підрозділів (замовлення, види ресурсів, виконанні поставлених задач);
- оптимізація потоків матеріальних ресурсів;
- скорочення надлишкових ресурсів на складах;
- скорочення невиробничих витрат;
- оперативне, короткострокове, середньострокове, довгострокове планування діяльності підприємства;
- планування й оперативний контроль за циклом виробництва для підвищення ефективності використання виробничих потужностей та ресурсів;
- створення гнучкої інформаційної системи у відділі реалізації продукції (контроль за платежами, відвантаженням продукції термінами виконання договірних зобов'язань);
- автоматизація фінансової діяльності і надання її результатів керівництву підприємства;
- зменшення сукупної вартості засобів інформаційних технологій;
- гнучка зміна системи залежно від потреб підприємства.

Для стандарту MRP II природним є використання ієрархічних планів, або залежності планів нижніх рівнів від планів більш високих рівнів шляхом відповідності заданим раніше показникам. Звязок планів має на увазі також і можливість зворотного впливу їх один на одного [6].

На рис. 2.3 представлений ланцюжок планів у відповідності зі стандартом MRPII.

Рис.1.3. Ланцюжок планів у стандарті MRP II

1.1.3. Організація інформаційних систем у відповідності до стандарту ERP

ERP-системи (Enterprise Resource Planning) називаються корпоративною надбудовою над MRP-системами, вони можуть використовуватися великими підприємствами для управління потоками даних та їх збереження. Якщо основна увага MRPII спрямована на керування виробничими ресурсами, то методи ERP претендують на керування всіма ресурсами, що маються у підприємства включаючи персонал, фінанси тощо. ERP краще враховує корпоративну структуру підприємства, його міжнародний масштаб. Та системи реалізують керування віддаленими підприємствами і збутовими підрозділами в усьому світі. Асоціація American Production and Inventory Control Socielj регламентує зміст сучасної системи керування підприємством, що відповідає концепції ERP у такий спосіб [5]:

1. Модуль управління ланцюжком постачань (Supply Chain Management – SCM, раніше – DRP (Distribution Resource Plannin)
2. Модуль удосконаленого планування і складання розкладів(Advanced Planning and Scheduling – APS)
3. Модуль автоматизації продажів (Sales Force Automation)
4. Автономний модуль, який відповідає за конфігурацію (Stan Alone Configuration Engine – SCE)
5. Модуль остаточного планування ресурсів (Finite Resourj Planning – FRP).
6. Модуль інтелект бізнесу, OL AP -технології (Busine] Intelligence - BI).
7. Модуль електронної комерції (Electronic Commerce - EC)
8. Модуль управління даними про виріб (Product Dal Management - PDM).

Так, сьогодні існують такі методики [6]:

□□□ $^{5}И''*''$ – вміщує ідеологію JIT (Just in Time) - «точно вчасно», елементи «канбансистем».

– CALS 1 (Computer Aided Logistic Support) - забезпечують комп'ютерну підтримку поставок.

- Extended ERP - забезпечують управління ланцюжками поставок або виконують Supply Chain, які дозволяють направляти та контролювати рух матеріальних та інформаційних потоків від відправника до одержувача.
- CALS 2 (Continuous Acquisition and Life cycle Support) - забезпечують безперервну інформаційну підтримку життєвого циклу продукту.
- CSRP (Customer Synchronized Resource Planning) - забезпечують інтеграцію покупця та підрозділів, які відносяться до процесу купівлі, із головними плановими та виробничими підрозділами; інтеграцію власних 1С із додатками клієнтів та постачальників; планування заказів покупців; покриття всього життєвого циклу продукту в інтегрованих інформаційних системах (ИС), інтеграцію в ПС CALS-технологій.

1.2. Аналіз проблеми управління привілейованим доступом у корпоративній інформаційній системі

Керування привілейованим доступом (PAM) складається із стратегій і технологій кібербезпеки для здійснення контролю над підвищеним («привілейованим») доступом і дозволами для користувачів, облікових записів, процесів і систем в IT-середовищі. Набираючи відповідний рівень привілейованого контролю доступу, PAM допомагає організаціям сконцентрувати поверхню атаки своєї організації та запобігти або, принаймні, пом’якшити шкоду, яка виникає від зовнішніх атак, а також від внутрішніх зловживань чи недбалості [7].

Хоча управління привілеями охоплює багато стратегій, головною метою є забезпечення мінімальних привілеїв, які визначаються як обмеження прав доступу та дозволів для користувачів, облікових записів, додатків, систем, пристроїв (наприклад, IoT) та обчислювальних процесів до абсолютного мінімуму, необхідного для виконувати рутинну, санкціоновану діяльність.

По-іншому, PAM, який також називають привілейованим керуванням обліковим записом, привілейованим керуванням ідентифікацією (PIM) або просто

керуванням привілеями, багато аналітиків і технологів вважають одним з найважливіших проектів безпеки для зниження кіберризиків і досягнення високої рентабельності інвестицій.

Загалом прийнято, що область керування привілеями входить до ширшої сфери управління ідентифікацією та доступом (IAM). Разом PAM та IAM допомагають забезпечити детальний контроль, видимість та можливість аудиту над усіма обліковими даними та привілеями.

У той час як елементи керування IAM забезпечують аутентифікацію ідентифікаційних даних, щоб гарантувати, що потрібний користувач має правильний доступ у потрібний час, PAM надає більш детальну видимість, контроль та аудит над привілейованими ідентифікаторами та діяльністю [7].

1.2.1. Визначення та процес створення «привілеїв».

Привілей у контексті інформаційних технологій можна визначити як повноваження, які має даний обліковий запис або процес у комп'ютерній системі чи мережі. Privilege надає дозвіл на скасування або обхід певних обмежень безпеки і може включати дозволи на виконання таких дій, як вимкнення систем, завантаження драйверів пристроїв, налаштування мереж або систем, надання та налаштування облікових записів і хмарних екземплярів тощо.

У своїй книзі Privileged Attack Vectors автори та лідери галузі Морі Хабер і Бред Хібберт (обидва з BeyondTrust) пропонують основне визначення; «Привілей — це особливе право чи перевага. Це піднесення над нормою, а не налаштування чи дозвіл, наданий масам».

Привілеї виконують важливу оперативну мету, надаючи користувачам, програмам та іншим системним процесам підвищені права на доступ до певних ресурсів і виконання пов'язаних з роботою завдань. У той же час можливість неправомірного використання або зловживання привілеями з боку інсайдерів або зовнішніх зловмисників створює для організацій серйозний ризик для безпеки.

Привілеї для різних облікових записів і процесів вбудовуються в операційні системи, файлові системи, програми, бази даних, гіпервізори, платформи управління хмарами тощо. Привілеї також можуть призначатися певними типами привілейованих користувачів, наприклад, системним або мережевим адміністратором.

Залежно від системи, деякі привілеї або делегування людям можуть ґрунтуватися на атрибутах, які залежать від ролі, наприклад, бізнес-підрозділ (наприклад, маркетинг, кадри чи IT), а також на ряді інших параметрів (наприклад, стаж, час доби, особливі обставини тощо) [7].

У середовищі з найменшими привілеями більшість користувачів працюють з непривілейованими обліковими записами 90-100% часу. Непривілейовані облікові записи, які також називають найменш привілейованими обліковими записами (LUA), загалом складаються з наступних двох типів:

Стандартні облікові записи користувачів мають обмежений набір привілеїв, наприклад, для перегляду в Інтернеті, доступу до певних типів програм (наприклад, MS Office тощо), а також для доступу до обмеженого набору ресурсів, які часто визначаються політикою доступу на основі ролей.

Облікові записи гостей мають менше привілеїв, ніж стандартні облікові записи користувачів, оскільки вони зазвичай обмежуються лише доступом до базових програм та переглядом Інтернету.

Привілейованим обліковим записом вважається будь-який обліковий запис, який надає доступ і привілеї, крім тих, що не є привілейованими обліковими записами. Привілейований користувач – це будь-який користувач, який наразі використовує привілейований доступ, наприклад, через привілейований обліковий запис. Через свої розширені можливості та доступ привілейовані користувачі/привілейовані облікові записи становлять значно більші ризики, ніж непривілейовані облікові записи/непривілейовані користувачі.

Спеціальні типи привілейованих облікових записів, відомі як облікові записи суперкористувачів, в основному використовуються для адміністрування спеціалізованими IT-спеціалістами і надають практично необмежені можливості

для виконання команд і внесення змін в систему. Облікові записи суперкористувачів зазвичай відомі як «Root» в Unix/Linux і «Адміністратор» у системах Windows [7].

Привілеї облікового запису суперкористувача можуть надавати необмежений доступ до файлів, каталогів і ресурсів з повними привілеями читання/запису/виконання, а також правом надавати системні зміни в мережі, наприклад створювати або інсталювати файли чи програмне забезпечення, змінювати файли та налаштування та видаляти. користувачів і даних. Суперкористувачі можуть навіть надавати та відкликати будь-які дозволи іншим користувачам. Якщо ці привілейовані облікові записи використані неправильно (наприклад, випадкове видалення важливого файлу або введення потужної команди) або зі зловмисним наміром, вони можуть легко завдати катастрофічної шкоди всій системі або навіть всьому підприємству.

У системах Windows кожен комп'ютер Windows має принаймні один обліковий запис адміністратора. Обліковий запис адміністратора дозволяє користувачеві виконувати такі дії, як встановлення програмного забезпечення та зміна локальних конфігурацій та налаштувань.

Mac OS X, з іншого боку, схожа на Unix, але на відміну від Unix і Linux рідко розгортається як сервер. Користувачі кінцевих точок Mac можуть працювати з root-доступом за замовчуванням. Однак, як найкраща практика безпеки, слід створити непривілейований обліковий запис і використовувати його для рутинних обчислень, щоб обмежити ймовірність та обсяг привілейованих загроз.

Ось приклади привілейованих облікових записів, які зазвичай використовуються в організації [7]:

- Локальні адміністративні рахунки.
- Неособисті облікові записи, що надають адміністративний доступ лише до локального хосту або екземпляра.
- Адміністративні облікові записи домену.

- Привілейований адміністративний доступ до всіх робочих станцій і серверів у домені.
- «Розбийте скло» (також називають аварійним або пожежним викликом) облікові записи.
- Непривілейовані користувачі з адміністративним доступом до захищених систем у разі надзвичайних ситуацій.
- Сервісні рахунки.
- Привілейовані локальні або доменні облікові записи, які використовуються програмою або службою для взаємодії з операційною системою.
- Облікові записи Active Directory або служби домену.
- Увімкнути зміну паролів до облікових записів тощо.
- Облікові записи додатків.

Використовується програмами для доступу до баз даних, виконання пакетних завдань або сценаріїв або надання доступу до інших програм.

Хоча більшість користувачів, які не належать до IT, як найкраща практика, повинні мати лише стандартний доступ до облікового запису користувача, деякі IT-службовці можуть мати кілька облікових записів, ввійти як звичайний користувач для виконання рутинних завдань, а також ввійти в обліковий запис суперкористувача для виконання адміністративних дій.

Оскільки облікові записи адміністратора мають більше привілеїв і, таким чином, становлять підвищений ризик у разі неправильного використання або зловживання в порівнянні зі стандартними обліковими записами користувачів, найкраща практика PAM полягає в тому, щоб використовувати ці облікові записи адміністратора лише тоді, коли це абсолютно необхідно та протягом найкоротшого часу.

Привілейовані облікові дані (також звані привілейованими паролями) — це підмножина облікових даних, які надають підвищений доступ і дозволи для

облікових записів, програм і систем. Привілейовані паролі можуть бути пов’язані з обліковими записами людей, програм, служб тощо. Ключі SSH — це один із типів привілейованих облікових даних, які використовуються на підприємствах для доступу до серверів і відкриття шляхів до високочутливих активів.

Іноді, особливо в середовищі DevOps, привілейовані облікові дані називають «секретами» [7].

Паролі привілейованих облікових записів часто називають «ключами до IT-царства», оскільки у випадку з паролями суперкористувача вони можуть надати автентифікованому користувачеві майже необмежені права привілейованого доступу до найважливіших систем і даних організації. Маючи таку велику силу, властиву цим привілеям, вони дозріли для зловживань з боку інсайдерів і дуже бажані хакерами. За оцінками Forrester Research, 80% порушень безпеки пов’язані з привілейованими обліковими даними.

1.2.1 Головні проблеми управління доступом та обліковими даними

Деякі з основних ризиків і проблем, пов’язаних із привілеями, включають:

1. Відсутність видимості та поінформованості про привілейованих користувачів, облікових записів, активів та облікових даних: давно забуті привілейовані облікові записи зазвичай поширені в різних організаціях.

   Ці облікові записи можуть нараховуватися мільйонами і є небезпечними бекдорами для зловмисників, у тому числі, у багатьох випадках, колишніх співробітників, які залишили компанію, але зберегли доступ.

2. Надмірне надання привілеїв: якщо засоби контролю привілейованого доступу є надмірно обмеженими, вони можуть порушити робочі процеси користувачів, спричинити розчарування та перешкоджаючи продуктивності.

Оскільки кінцеві користувачі рідко скаржаться на занадто багато привілеїв, IT-адміністратори традиційно надають кінцевим користувачам широкий набір привілеїв. Крім того, роль співробітника часто мінлива і може розвиватися таким чином, що вони накопичують нові обов'язки та відповідні привілеї, зберігаючи при цьому привілеї, які вони більше не використовують або не потребують [7].

Весь цей надлишок привілеїв призводить до роздутої поверхні атаки. Регулярні обчислення для співробітників на персональних ПК можуть включати в себе перегляд Інтернету, перегляд потокового відео, використання MS Office та інших базових програм, включаючи SaaS (наприклад, Salesforce.com, GoogleDocs тощо). У випадку ПК з Windows користувачі часто входять в систему з правами адміністратора — набагато ширшими, ніж це необхідно. Ці надмірні привілеї значно збільшують ризик того, що зловмисне програмне забезпечення або хакери можуть викрасти паролі або встановити шкідливий код, який може бути доставлений через веб-серфінг або вкладення електронної пошти. Зловмисне програмне забезпечення або хакер може використовувати весь набір привілеїв облікового запису, отримати доступ до даних зараженого комп'ютера і навіть запустити атаку на інші мережеві комп'ютери або сервери.

3. Спільні облікові записи та паролі: IT-команди зазвичай використовують root, адміністратор Windows та багато інших привілейованих облікових даних для зручності, тому робочі навантаження та обов'язки можна легко розподіляти за потреби. Однак, оскільки кілька людей використовують пароль облікового запису, може бути неможливо прив'язати дії, виконані з обліковим записом, з однією особою. Це створює проблеми з безпекою, аудитом і відповідністю [7].

4. Жорстко запрограмовані / вбудовані облікові дані: привілейовані облікові дані необхідні для полегшення автентифікації для зв'язку та доступу між програмою та базою даних (A2A) та програмою з базою даних (A2D).

Додатки, системи, мережеві пристрої та пристрої Інтернету речей зазвичай поставляються — і часто розгортаються — із вбудованими обліковими даними за

замовчуванням, які легко вгадати та становлять значний ризик. Крім того, співробітники часто твердо кодують секрети у вигляді простого тексту, наприклад, у сценарії, коді або файлі, щоб вони були легко доступні, коли їм це потрібно.

5. Ручне та/або децентралізоване керування обліковими даними: засоби контролю безпеки привілеїв часто є незрілими. Керування привілейованими обліковими записами та обліковими даними в різних організаційних підрозділах може здійснюватися по-різному, що призводить до непослідовного застосування найкращих методів роботи.

Процеси керування привілеями людини неможливо масштабувати в більшості IT-серед, де можуть існувати тисячі або навіть мільйони привілейованих облікових записів, облікових даних та активів. З такою кількістю систем і облікових записів, якими можна керувати, люди завжди користуються ярликами, наприклад повторно використовують облікові дані для кількох облікових записів і активів. Таким чином, один зламаний обліковий запис може поставити під загрозу безпеку інших облікових записів із такими ж обліковими даними [7].

6. Відсутність видимості привілеїв облікових записів додатків і служб: програми та облікові записи служб часто автоматично виконують привілейовані процеси для виконання дій, а також для зв’язку з іншими програмами, службами, ресурсами тощо.

Програми та облікові записи служб часто мають надмірні права привілейованого доступу через за замовчуванням, а також страждають від інших серйозних недоліків безпеки.

7. Інструменти та процеси керування ідентифікаційними особами ізольовано: сучасні IT-середовища зазвичай працюють на кількох платформах (наприклад, Windows, Mac, Unix, Linux тощо), кожна з яких підтримується та керується окремо.

Така практика прирівнюється до непослідовного адміністрування IT, додаткової складності для кінцевих користувачів і підвищеного кіберризику.

IoT, DevOps і хмарні середовища представляють нові привілейовані вектори загроз і варіанти використання керування привілеями [7]:

- Хмарні консолі та консолі адміністратора віртуалізації (наприклад, AWS, Office 365 тощо) надають майже безмежні можливості суперкористувача, дозволяючи користувачам швидко надавати, налаштовувати та видаляти сервери у великих масштабах. На цих консолях користувачі можуть без зусиль розкручувати тисячі віртуальних машин і керувати ними (кожна зі своїм набором привілеїв і привілейованих облікових записів). Організаціям потрібен належний привілейований контроль безпеки, щоб інтегрувати та керувати всіма цими нещодавно створеними привілейованими обліковими записами та обліковими даними у масовому масштабі.
- Середовища DevOps — з їхнім наголосом на швидкості, розгортанні хмари й автоматизації — створюють багато проблем і ризиків щодо керування привілеями. Організації часто не бачать привілеїв та інших ризиків, пов’язаних із контейнерами та іншими новими інструментами. Неадекватне керування секретами, вбудовані паролі та надмірне надання привілеїв — це лише кілька ризиків, пов’язаних із привілеями, поширеними серед типових розгортань DevOps.
- Пристрої IoT зараз широко поширені на підприємствах. Багато IT-команд намагаються виявити та безпечно встановити на борту законні пристрої в масштабі. Посилюючи цю проблему, пристрої IoT зазвичай мають серйозні недоліки безпеки, такі як жорстко закодовані паролі за замовчуванням і неможливість посилити програмне забезпечення або оновити мікропрограму.

1.3. Мета та завдання управління привілейованим доступом у корпоративній інформаційній системі

Хакери, зловмисне програмне забезпечення, партнери, інсайдери, які стали шахраями, і прості помилки користувачів, особливо у випадку облікових записів суперкористувачів, є найбільш поширеними векторами привілейованих загроз.

Зовнішні хакери прагнуть отримати привілейовані облікові записи та облікові дані, знаючи, що після отримання вони забезпечують швидкий шлях до найкритичніших систем і конфіденційних даних організації. Маючи в руках привілейовані облікові дані, хакер, по суті, стає «інсайдером» — і це небезпечний сценарій, оскільки вони можуть легко стерти свої сліди, щоб уникнути виявлення під час проходження скомпрометованого IT-середовища.

Хакери часто закріплюються за допомогою низькорівневого експлойту, наприклад, за допомогою фішингової атаки на стандартний обліковий запис користувача, а потім проходять через мережу, доки не знайдуть бездіяльний або осиротілий обліковий запис, що дозволяє їм посилити свої привілеї [7].

На відміну від зовнішніх хакерів, інсайдери вже починають з периметра, а також отримують вигоду від ноу-хау про те, де лежать конфіденційні активи та дані та як їх зосередити. Найдовше розкриваються інсайдерські загрози, оскільки працівники та інші інсайдери зазвичай отримують певний рівень довіри за замовчуванням, що може допомогти їм уникнути виявлення. Тривалий час до відкриття також призводить до більш високого потенціалу шкоди. Багато з найбільш катастрофічних порушень за останні роки були скоєні інсайдерами.

Чим більше привілеїв і доступу накопичено у користувача, облікового запису або процесу, тим більша ймовірність зловживання, використання або помилки. Реалізація керування привілеями не тільки мінімізує ймовірність порушення безпеки, але й допомагає обмежити масштаби порушення, якщо воно станеться [7].

Однією з відмінностей між PAM та іншими типами технологій безпеки є те, що PAM може демонтувати кілька точок ланцюга кібератак, забезпечуючи захист як від зовнішніх атак, так і від атак, які здійснюють його всередині мереж і систем.

PAM надає кілька основних переваг, зокрема:

- Згущена поверхня атаки, яка захищає як від внутрішніх, так і від зовнішніх загроз: обмеження привілеїв для людей, процесів і програм означає, що шляхи та входи для експлойту також зменшуються.
- Зменшення зараження та поширення зловмисного програмного забезпечення: багато різновидів шкідливих програм (наприклад, ін'єкції SQL, які покладаються на відсутність найменших привілеїв) потребують підвищених привілеїв для встановлення або виконання. Видалення надмірних привілеїв, наприклад, шляхом мінімального застосування привілеїв на підприємстві, може запобігти поширенню зловмисного програмного забезпечення або зменшити його поширення, якщо це станеться.
- Підвищення продуктивності роботи: обмеження привілеїв мінімальним набором процесів для виконання дозволеної діяльності зменшує ймовірність проблем несумісності між програмами чи системами та допомагає зменшити ризик простою.
- Легше досягти та підтвердити відповідність: обмежуючи привілейовані дії, які можуть бути виконані, керування привілейованим доступом допомагає створити менш складне, а отже, більш зручне для аудиту середовище [7].

Крім того, багато правил відповідності (включаючи HIPAA, PCI DSS, FDDC, Government Connect, FISMA і SOX) вимагають, щоб організації застосовували політику доступу з найменшими привілеями для забезпечення належного

управління даними та безпеки систем. Наприклад, у мандаті FDCC федерального уряду США зазначено, що федеральні службовці повинні входити на ПК зі стандартними правами користувача.

1.4. Аналіз існуючих технологій управління привілейованим доступом у корпоративній інформаційній системі

Інструменти керування привілейованим доступом є важливою частиною більш широкої програми кібербезпеки. Вони допомагають організаціям [8]:

- Відкрити для себе всі облікові записи, які мають адміністративні привілеї для локальних і хмарних робочих навантажень, включаючи облікові записи, які використовуються окремими особами, і привілейовані облікові дані «від машини до машини».
- Мінімізувати ризики, пов’язані з неналежним адміністративним доступом.
- Досягнути та підтвердити відповідність галузевим і нормативним вимогам.

Традиційні рішення для керування привілейованим доступом зазвичай працюють так:

1. Користувач, якому потрібно виконати завдання, що вимагає підвищених дозволів, запитує доступ до привілейованого облікового запису, пояснюючи, чому йому потрібен привілейований доступ.
2. Рішення PAM автоматично схвалює запит відповідно до політики або за бажанням направляє його відповідному менеджеру для затвердження вручну.
3. Коли схвалення надано, рішення PAM реєструє рішення і надає користувачеві тимчасовий привілейований доступ, необхідний для

виконання зазначеного завдання. Зазвичай вони отримують доступ через PAM замість того, щоб дізнатися пароль для привілейованого облікового запису [8].

Можна сформулювати основні критерії адекватності програмного комплексу щодо управління привілейованим доступом:

1. Рішення має дозволяє керувати сесіями для привілейованих дій з будь-якого браузера, будь-якої ОС.

Сучасний ландшафт користувачів розвивається разом із динамічними змінами безпеки операційних систем і браузерів. Якщо використовуються старі й обмежені методи керування сеансами на основі Active-x / Java, треба негайно оцінити виправлення безпеки.

2. Можливості адміністрування PAM мають надаватися через веб-браузер без будь-яких завантажень сторонніх клієнтів в уніфікованій консолі керування.

Робота з товстими клієнтами вимагає надання прямого доступу до сховища та даних конфігурації. Кілька консолей і товстих клієнтів часто вимагають виправлення кількох систем, залишаючи вразливість невиправлених систем.

3. Має бути створений доступний механізм на основі правил, який дозволяє адміністраторам створювати правила для визначення динамічних привілейованих груп облікових записів на основі членства в AD, відділів, типів активів для єдиного керування політикою.

Покладаючись на ручне втручання для створення політик не тільки сповільнює впровадження, але й збільшує ймовірність помилок і навіть надмірних привілеїв.

4. Мають бути автоматизовані рутинні привілейовані завдання, щоб дотримуватись нульової довіри.

Покладаючись на ручне втручання для створення політик не тільки сповільнює впровадження, але й збільшує ймовірність помилок і навіть надмірних привілеїв.

5. Організоване безпечне керування ключами SSH і ключами доступу.

Якщо регулярно надається привілейований доступ постачальникам або користувачам для кожної рутинної діяльності, надаються надмірні привілеї та виявляються потенційні прогалини в безпеці.

6. Організована безпечна платформа привілейованих облікових записів з можливостями автоматичного посилення без необхідності сторонніх СУБД.

Організації все частіше дозволяють використовувати ключі SSH, щоб уникнути ризику керування паролями та їх передачі. Ключі SSH для доступу до пристроїв і ключі доступу для керування хмарними консолями важливі для керування повною дорожньою картою проекту привілейованого облікового запису.

7. Налаштовані свої ключі шифрування, для виключного владіння привілейованими паролями.

Зовнішня СУБД збільшує витрати на керування кількома сценаріями та виправленнями для різних компонентів рішення. Одна інклюзивна платформа зменшує ручні зусилля при управлінні всіма компонентами рішення та мінімізує можливість помилок вручну під час регулярних виправлень і оновлень.

8. Інтегровані внутрішні або сторонні програми під платформу PAM без необхідності писати код.

Якщо немає доступу до ключа шифрування або немає можливості налаштувати свій ключ шифрування, є ризик отримати викуп у постачальника, який контролює ключ шифрування всіх критичних даних.

9. Налагоджене керування та відстеження віддаленого доступу постачальників без необхідності сторонніх плагінів.

Надання віддаленого доступу внутрішнім або зовнішнім користувачам передбачає надання кількох рівнів доступу. Оскільки машини постачальників є ненадійними джерелами, треба переконатися, що ці машини ізольовані від інформаційного середовища організації. Важливо мати можливості PAM, які можуть забезпечити ізоляцію сеансу без погіршення продуктивності.

10. Активи й облікові записи в хмарних та локальних місцях мають постійно виявлятися й керуватися.

Чим довше очікується, щоб активи та облікові записи з рішенням керування паролями були включені, тим вище схильність інформаційної системи до атак.

Висновки до розділу 1

В даному розділі було розглянуто основні особливості корпоративних інформаційних систем, досліджено головні проблеми забезпечення управління привілейованим доступом та розглянуто особливості сучасних технологій щодо управління привілейованим доступом.

Сформульовано основі критерії оцінки програмних комплексів управління привілейованим доступом в корпоративній системі.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ IBM SECURITY VERIFY PRIVILEGE VAULT

2.1. Призначення, можливості та функції IBM Security Verify Privilege Vault

Привілейований доступ — це шлях до найціннішої інформації організації. В результаті впровадження управління привілейованим доступом (PAM) стало головним пріоритетом.

IBM Security Verify Privilege Vault — це повнофункціональне PAM-рішення, доступне як локально, так і в хмарі, готове надати вашій команді з питань безпеки та IT-операцій швидко й легко захищати й керувати всіма типами привілейованих облікових записів.

Технологія Verify Privilege Vault надає можливість :

- Створити безпечне сховище – зберігання привілейованих облікових даних в зашифрованому централізованому сховищі.
- Дізнатися про привілеї – Визначення всіх облікових записів служб, програм, адміністратора та root.
- Захист паролів. Автоматизування зміни паролів, забезпечення складності паролів і змінення облікових даних.
- Відповідність вимогам – активна відповідність за допомогою аудиту, звітності та сповіщень.
- Контрольні сеанси – реалізуйте запуск сеансу, проксі, моніторинг та запис.
- Моніторинг активності – відстеження підозрілих та нерегулярних моделей діяльності за допомогою додаткового модуля Analytics. Перевірка, що

сховище привілеїв швидке в розгортанні, просте у використанні та масштабоване для підприємства. Він інтегрується з більшим портфоліо IBM Security для ключових випадків використання, таких як керування ідентифікацією та багатофакторна аутентифікація. Підтримка IBM доступна цілодобово. Також доступні рекомендації щодо розгортання, консультації зі стратегії та керовані PAM-сервіси [9].

2.2. Компоненти та архітектура рішення IBM Security Verify Privilege Vault

IBM надає комплексні можливості PAM через рішення корпоративного рівня: IBM Security Verify Privilege Vault і IBM Security Verify Privilege Manager. Завдяки консультаціям експертів і підтримці 24/7, Verify Privilege Vault і IBM Privilege Manager допомагають отримати вигоду з усього, що може запропонувати PAM, а також інтегрується з рішеннями щодо керування ідентифікацією для повного керування життєвим циклом для користувачів привілейованих облікових записів.

Ключовою частиною безпеки організації є забезпечення інтеграції особистих даних у ширшу екосистему безпеки, щоб пом’якшити внутрішні та зовнішні загрози. Дві ключові частини цього:

- Управління привілейованим доступом – зосереджено на особливих вимогах для управління потужними обліковими записами в IT-інфраструктурі підприємства.
- Privileged Elevation and Delegation Management (PEDM) – який запобігає зовнішнім загрозам і зупиняє використання програм зловмисним програмним забезпеченням і вимагачем, видаляючи локальні адміністративні права з кінцевих точок.

Вони складаються з наступних компонентів:

1. Знаходження, контроль, зміна та перевірка привілейованих облікових записи.

Першим кроком в управлінні привілейованими обліковими записами є пошук облікових записів, про існування яких невідомо. Ручні процеси та помилки можуть призвести до облікових записів, які невідомі та некеровані IT. За допомогою IBM Security Verify Privilege Vault є можливість автоматично сканувати всю свою IT-інфраструктуру, щоб виявити привілейовані, спільні та службові облікові записи. Ця конфіденційна інформація потім зберігається в зашифрованому централізованому сховищі для забезпечення належного захисту за допомогою передових стандартів шифрування. Політику щодо паролів можна запровадити та застосувати для кожного облікового запису. Можливо отримувати повну видимість і контроль над кожним привілейованим обліковим записом у інформаційному середовищі [9].

2. Обмеження поширення привілейованого доступу.

При виявленні всіх привілейованих облікових записів у інфраструктурі за допомогою технології Verify Privilege Vault, ідентифікуються всі облікові записи служб, програм, адміністратора та root. Це означає, що можливо отримувати повну видимість і контроль над привілейованими обліковими даними, які раніше залишалися непоміченими.

3. Генерація, зберігання, вибір та керування ключами SSH

Є можливість перенести генерацію, обертання, контроль і захист ключів SSH безпосередньо в Verify Privilege Vault. Ключі SSH подібні до імен користувачів і паролів, але використовуються для автоматизованих процесів і для реалізації єдиного входу системними адміністраторами. За допомогою контролю доступу на

основі ролей і наборів дозволів можливо контролювати, хто має доступ до яких наборів ключів, незалежно від розташування чи IP-адреси.

4. Відстежування та запис привілейованих сеансів.

IBM Security Verify Privilege Vault дає змогу відстежувати сеанси в реальному часі та дозволяє завершити сеанс у разі виявлення ризикованої поведінки. Технологія також дозволяє записувати активність привілейованих користувачів. Це забезпечує контрольний слід від того, коли користувач перевіряє секрет, до того, що він зробив у системі, до того, коли він нарешті вийшов. Можна отримати повне уявлення про те, що відбувається у найважливіших облікових записах.

5. Автоматичне змінення паролів, коли термін їх дії закінчується.

Привілейовані паролі слід регулярно змінювати. Можна переконатися, що вбудований у Privilege Vault графік зміни та закінчення терміну дії паролів гарантує, що важливі паролі змінюються автоматично, без ручного втручання.

6. Делегування доступу до всіх привілейованих облікових записів.

Підтримання підзвітності і забезпечення кращого контексту для схвалювачів, щоб вони точно знали, чому користувачеві потрібен доступ. Також можна налаштувати контроль доступу на основі ролей (RBAC) і робочий процес затвердження, який забезпечує прозорий доступ, обмеження за часом та інші параметри цього доступу та затвердження пароля для третіх сторін [9].

7. Розширений аудит та звітність.

Використання десятка готових звітів для кращого розуміння стану системи та її відповідності. Є можливість створювати повні звіти про активність сховищ паролів і створювати власні звіти із запитів до бази даних, якщо це необхідно.

8. Інтегрування IBM Security Verify Privilege Vault для підвищення безпеки.

Технологія IBM Security Verify Privilege Vault легко інтегрується з критичними рішеннями IBM Security, включаючи IBM Cloud Identity, QRadar, Guardium Data Protection і IBM Security Identity Governance & Intelligence [9].

2.3 Вимоги до системи для інсталяції IBM Security Verify Privilege Vault

2.3.1 Системні вимоги

Мінімальні вимоги для базового розгортання (табл. 2.1):

Табл. 2.1 Мінімальні вимоги для базового розгортання IBM Security Verify Privilege Vault

Web Server	Database Server
2 CPU Cores	2 CPU Cores
4 GB RAM	4 GB RAM
25 GB Disk Space	50 GB Disk Space
Windows Server 2012	Windows Server 2012
IIS 7 or newer (64-bit applications only)	SQL Server 2012-2019
.NET 4.8 or newer	Collation SQL_Latin1_General_CP1_CI_AS

Рекомендовані вимоги до базового розгортання:

Табл. 2.1 – Рекомендовані вимоги для базового розгортання IBM Security Verify Privilege Vault

Web Server	Database Server
4 CPU Cores	4 CPU Cores
16 GB RAM	16 GB RAM
25 GB Disk Space	100+ GB Disk Space
Windows Server 2012-2019	Windows Server 2012-2019
IIS 7 or newer (64-bit applications only)	SQL Server 2012-2019
.NET 4.8 or newer	Collation SQL_Latin1_General_CP1_CI_AS

Щоб відповідати вимогам ліцензування Microsoft, існує додаткове обмеження щодо того, яку версію Microsoft Windows Server можна використовувати як сервер RDS для з'єднувача сеансу [10].

Якщо використовується ліцензії клієнтського доступу користувача Microsoft (CAL), неможливо використовувати Windows Server 2019. Необхідно використовувати Windows Server 2012 або 2016. Якщо використовується ліцензія Microsoft Device CAL, можливо використовувати будь-яку підтримувану версію Windows Server.

Verify Privilege Vault вимагає, щоб Microsoft SQL Server і його база даних були встановлені на параметр зіставлення SQL_Latin1_General_CP1_CI_AS. Системні вимоги стосуються як фізичних, так і віртуальних машин.

Для найкращої продуктивності рекомендується використовувати виділені (чисті) сервери для розміщення продуктів IBM Security.

Якщо функції .NET або IIS ще не встановлені на веб-сервері, IBM Security Installer додасть і налаштує їх автоматично.

Якщо SQL ще не встановлено на сервері баз даних, інсталятор IBM Security може налаштувати SQL Express на веб-сервері; однак SQL Express призначений лише для пробних і пісочниць. Хоча IBM Security підтримуватиме SQL Express, користувачі, ймовірно, відчуватимуть проблеми з продуктивністю через обмеження пам'яті та продукту. Якщо під час використання SQL Express

виникають проблеми з продуктивністю, настійно рекомендується оновити SQL Server до SQL Server перед тим, як звертатися до служби підтримки безпеки IBM.

Встановлення Verify Privilege Vault за допомогою Azure SQL: наразі ми не рекомендується використовувати Verify Privilege Vault з Azure SQL, якщо веб-хост і екземпляр Azure SQL знаходяться в різних центрах обробки даних. За даними Microsoft, програми, такі як Verify Privilege Vault, які використовують часті, великі спеціальні запити, використовують значний час відповіді на мережевий зв'язок між програмою та рівнями бази даних Azure SQL. Таким чином, затримка мережі під час багатьох операцій доступу до даних у центрах обробки даних може стати проблемою.

Непідтримувані веб-сервери: Small Business Server (SBS), The Essentials Edition, будь-які клієнтські ОС, контролери домену, сервери SharePoint.

Verify Privilege Vault Cloud вимагає локальної машини для використання розподіленого механізму.

Програми запуску SQL не підтримують SSMS 18.0 або новішої версії.

Сканування виявлення для запланованих завдань Windows Server 2016 вимагає, щоб вузол Verify Privilege Vault або розподілений механізм, який виконує сканування, працював на Windows Server 2016 або новішої версії. Це пов'язано зі змінами в Windows Server 2016 API, який використовується для сканування залежностей за розкладом [10].

AWS RDS: наразі не рекомендується використовувати Verify Privilege Vault з AWS Relational Database Service, якщо веб-хост і екземпляр SQL знаходяться в різних центрах обробки даних. Додатки, такі як Verify Privilege Vault, які використовують часті, інтенсивні спеціальні запити, залежать від швидкого часу реакції мережевого зв'язку між програмою та базою даних SQL. Таким чином, затримка мережі під час багатьох операцій доступу до даних у центрах обробки даних може стати проблемою.

Verify Privilege Vault вимагає, щоб пул програм мав увімкнений параметр «завантаження профілю користувача». Verify Privilege Vault повідомить про

критичне сповіщення, щоб сповістити адміністраторів, якщо цей параметр не ввімкнено.

Підтримувані веб-браузери:

- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge. Лише Edge Chromium. Застарілий Microsoft Edge не підтримується;
- Safari;
- Microsoft Internet Explorer 11 (підтримка Internet Explorer 11 припиниться 31 серпня 2021 року).

2.3.2 Вимоги до обладнання

SS можна встановити на фізичному сервері або віртуальній машині. Якщо необхідно налаштувати кластеризацію інтерфейсу (програми), потрібно мати два або більше доступних серверів.

Для тестування високої доступності для SQL Server можна використовувати існуючу інфраструктуру Microsoft AlwaysOn або дзеркальне відображення бази даних [10].

2.3.3 Вимоги до програмного забезпечення

- Windows Server 2012 або новішої версії (рекомендовано) (мінімум один сервер);
- SQL Server (один екземпляр, мінімум);
- Передумови сервера програм;
- SSL сертифікат;

– SQL Server.

Присутня можливість створити базу даних SQL в існуючому екземплярі SQL або в новій інсталяції SQL Server. Для високої доступності це має бути платна версія SQL Server (не SQL Express).

– Сервер додатків.

Рекомендується встановити Verify Privilege Vault на Windows Server 2012 або новішої. Включіть IIS, ASP.NET і .NET Framework [10].

2.3.4 Конфігурація програми

– Сервісний обліковий запис.

Для налаштування облікового запису служби необхідно:

1. Увійти як пакетне завдання (на сервері, на якому працює Verify Privilege Vault);
2. Змінити дозволи до каталогу програм Verify Privilege Vault (зазвичай C:\inetpub\wwwroot) і C:\Windows\temp;
3. Надати доступ до екземпляра SQL Server, додавши дозвіл db_owner до бази даних Verify Privilege Vault.

Для тестування функцій, які покладаються на Active Directory, наприклад, синхронізацію групи AD або виявлення, потрібно мати доступні облікові записи з відповідними дозволами (описані нижче). Один із варіантів — використовувати один обліковий запис для обох функцій.

– Групова синхронізація Active Directory.

Синхронізація групи Active Directory означає, що Verify Privilege Vault може автоматично додавати користувачів і дозволяти або виключати їх вхід до Verify

Privilege Vault на основі їхнього членства в групі Active Directory. Можна вибрати, які групи синхронізувати. Під час налаштування синхронізації групи AD в Verify Privilege Vault потрібно вказати обліковий запис, який може читати властивості користувачів і груп [10].

– Відкриття.

Щоб перевірити виявлення, підкажіть кілька комп'ютерів для підключення Verify Privilege Vault для виявлення облікових записів. Обліковий запис необхідний для синхронізації з AD, а також для сканування знайдених машин для виявлення локального облікового запису Windows і облікового запису служби. Дозволи облікового запису для виявлення описує дозволи, необхідні для використання облікового запису AD для виявлення.

– Тестові облікові записи.

Рекомендується мати кілька доступних тестових облікових записів, щоб представляти типи облікових записів, якими буде треба керувати за допомогою Verify Privilege Vault. Це можуть бути локальні облікові записи Windows, облікові записи служб, які виконують заплановані завдання або служби, облікові записи SQL-сервера та інші.

– Сповіщення електронною поштою.

Щоб перевірити сповіщення електронною поштою, які можна використовувати для сповіщень про підписку на події або запитів на підтвердження паролів, потрібна інформація про конфігурацію SMTP-сервера компанії:

1) Обліковий запис служби для запуску програми та підключення до SQL.
2) Домен (тестовий або робочий).
3) Обліковий запис домену, який буде використовуватися для синхронізації та виявлення AD.

4) Тестові машини (якщо тестування виявлення).
5) Тестові рахунки.
6) Налаштування SMTP-сервера.
7) Сертифікат SSL.

Рекомендується налаштувати SSL (або https) для доступу до Verify Privilege Vault. Для цього знадобиться сертифікат SSL. Можливо використовувати наявний сертифікат із підстановкою, створити власний сертифікат домену або придбати сторонній сертифікат SSL для Verify Privilege Vault [10].

– Брандмауери та порти.

SS повинен підключитися безпосередньо до цільової системи, щоб змінити свій пароль. Для пристроїв, які захищено брандмауером від Verify Privilege Vault, віддалений агент може забезпечити з'єднання з ними, але вони також потребують підключення до цільових систем для зміни пароля.

Висновки до розділу 2

В даному розділі розглянуто програмний комплекс IBM Security Verify Privilege Vault на основі документації розробника. Вказано вимоги та особливості його розгортання на базі корпоративної інформаційної системи. Сформульовані кроки для базової конфігурації програмного комплексу.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ IBM SECURITY VERIFY PRIVILEGE VAULT

3.1 Розроблення варіанта конфігурації системи управління привілейованим доступом в корпоративній інформаційній системі на базі IBM Security Verify Privilege Vault

На основі документації розробника щодо управління привілейованим доступом, присутній варіант базової конфігурації IBM Security Verify Privilege Vault:

1) Встановлення облікового запису адміністратора безпеки:

Адміністратор інформаційної безпеки – фахівець з питань інформаційної безпеки, призначений внутрішнім документом організації для забезпечення впровадження та підтримки роботи засобів захисту інформації.

Це перший обліковий запис, який буде створено під час процесу встановлення. Необхідно зберегти цей обліковий запис у безпеці та не заблокувати доступ до Verify Privilege Vault, дотримуючись порад [10]:

- Зберігати облікові дані в захищеному місці, до якого можна легко отримати доступ, якщо втрачається будь-який доступ до Verify Privilege Vault.
- Увімкнути параметр «Дозволити користувачам скидати забуті паролі», щоб забезпечити спосіб скидання пароля, якщо обліковий запис заблоковано або якщо пароль забутий:

а) Обрати «Адміністратор > Конфігурація». З'явиться сторінка конфігурації.
б) Натиснути вкладку «Локальні паролі користувачів», щоб знайти налаштування.
в) Натиснути кнопку «Редагувати», щоб відредагувати налаштування.
г) Після завершення натиснути кнопку «Зберегти».

– Налаштувати інші параметри паролів локальних користувачів, щоб забезпечити вимоги до паролів, термін дії, історію паролів та інші правила паролів.

2) Конфігурація SSL (HTTPS):

Рекомендується забезпечення SSL-доступу до Verify Privilege Vault. Для цього потрібно налаштувати SSL-сертифікат для веб-сайту, бажано із сертифікатом домену. Отримавши сертифікат необхідно:

– Налаштувати прив’язування HTTPS для веб-сайту Verify Privilege Vault за допомогою вибраного сертифіката.
– Переконатися, що сертифікат є надійним на машинах користувачів Verify Privilege Vault.
– Увімкнути «Примусовий HTTPS/SSL» на вкладці «Безпека» параметрів «Перевірка конфігурації сховища привілеїв».

3) Налаштування резервного копіювання задля уникнення втрати даних [10]:

Verify Privilege Vault надає можливість автоматичного створення резервної копії через визначений інтервал, надсилаючи дані в локальне або мережеве розташування.

Присутні два компоненти всієї резервної копії Verify Privilege Vault: файли веб-програми та база даних.

Знайти ці налаштування можна, вибравши «Резервне копіювання» в меню адміністратора.

4) Налаштування Verify Privilege Vault Framework:

Для роботи з Verify Privilege Vault, треба створити папки, ролі, користувачів і секрети для роботи:

- Рекомендується налаштувати структуру папок і кілька ролей. Структура папок – це спосіб упорядкування ваших секретів і доступ до спільних секретів. Крім того, ролі забезпечують можливість контролювати доступ до різних частин Verify Privilege Vault і призначати дозволи на перегляд певних папок і секретів.
- Додати користувачів, за умови, якщо AD не використовується.
- Додати Active Directory або інші секрети. Якщо використовується моніторинг, обліковому запису також знадобляться дозволи для перевірки комп'ютерів у мережі на наявність облікових записів.

5) Панель «Discovery»:

SS має функцію виявлення, яка може автоматично знаходити локальні облікові записи Windows, службу Active Directory, Unix, VMware ESX/ESXi та облікові записи домену Active Directory. Типи облікових записів і залежностей, які не підтримуються в SS із коробки, все ще можна виявити, написавши сценарії PowerShell, які можна запускати як спеціальні сканери. Це дозволяє адміністраторам швидко імпортувати облікові записи, знайдені SS, у визначених доменах або IP-адресах.

Щоб запустити виявлення в домені, діапазоні IP-адрес або спеціальному джерелі, спочатку потрібно увімкнути функцію виявлення для SS. Далі треба ввімкнути виявлення для кожного джерела виявлення, яке необхідно перевірити [10].

6) Налаштування віддалену зміну пароля:

Віддалена зміна пароля SS (RPC) надає можливість або почати зміну пароля вручну, або запланувати автоматичну зміну пароля через регулярні проміжки часу.

RPC вмикається на сторінці Адміністрування, Віддалена зміна пароля. Треба натиснути «Редагувати», щоб увімкнути RPC, секретний пульс і секретний контроль. Після ввімкнення всі секретні шаблони з налаштованим RPC доступні для використання з RPC.

7) Налаштування «Heartbeat»:

Heartbeat дає змогу визначити з Verify Privilege Vault, чи успішно автентифікуються облікові дані в секретній системі з цільовою системою. За замовчуванням функцію вимкнено в Verify Privilege Vault.

8) Налаштування аудитів та звітності:

Перш ніж запускати звіти та аудит, необхідно створити щось для звітування, з цією метою потрібно:

- Імпортувати кілька облікових записів або створити секрети вручну.
- Повернути паролі кілька разів.
- Переглянути декілька секретів.

Це генерує достатню кількість журналів аудиту, щоб забезпечити значущі результати у ваших звітах:

- Звіт про посилення безпеки.
- До яких секретів вдалося отримати доступ.
- Які таємниці провалили тест-серцебиття.
- Невдалі спроби входу.
- Секретна діяльність.

9) Налаштування сеансів запису:

Запис сеансу забезпечує додатковий рівень безпеки, записуючи дії користувача після використання запуску. Запис сеансу працює для будь-якої програми запуску, включаючи PuTTY і SSH, віддалений робочий стіл Windows, Microsoft SQL Management Studio і спеціальні виконувані файли. Існує два типи запису сеансу [10]:

- Базовий запис сеансу.
- Розширений запис сеансу.

Базовий запис сеансу є ліцензованою функцією в Verify Privilege Vault. Він покладається на обробник протоколу, налаштований на клієнтських машинах за допомогою програми запуску SS. За допомогою програми запуску Verify Privilege Vault робить посекундні знімки екрана на клієнтській машині під час записаного сеансу користувача. Ці зображення екрана користувача об’єднані у відео, яке можна завантажити та відтворити з метою аудиту та безпеки. Активність, записана під час сеансу, ґрунтується лише на змінах екрана.

Моніторинг сеансів дозволяє адміністраторам з дозволом на моніторинг сеансів переглядати всі активні запущені сеанси в Verify Privilege Vault. Якщо запис

сеансу увімкнено на секретному, адміністратор може спостерігати за сеансом користувача в режимі реального часу.

Адміністратори можуть здійснювати пошук серед активних і закінчених сеансів. Щоб переглянути та здійснити пошук серед сеансів, треба перейти у панель Адміністратор > Моніторінг сеансів.

Розширений запис сеансу (ASR) — це ліцензована функція Verify Privilege Vault, яка додає можливості до тих, які пропонує базовий запис сеансу. Присутня можливість Advanced Session Recording Agent (ASRA), який використовує протокол віддаленого робочого столу, на будь-якому клієнтському комп'ютері, де потрібно більше інформації про записані сеанси [10].

3.2 Технологія управління програмним комплексом IBM Security Verify Privilege Vault

У цьому розділі показано технологію управління IBM Security Verify Privilege Vault на прикладі найпоширеніших проблем в більшості підприємств.

3.2.1 Виявлення привілейованих облікових записів

Найчастіше організації навіть не знають, що вони мають привілейовані облікові записи і де вони зберігаються. Тому вони не можуть захистити ці облікові записи від хакерських або інсайдерських атак.

За допомогою Verify Privilege Vault, в якому реалізована функція виявлення, ці облікові записи будуть автоматично знайдені та перенесені до захищеного сховища для гарантії безпеки та нормативної відповідності.

Пошук невідомих привілейованих акаунтів відбувається через панель Discovery Verify Privilege Vault [11].

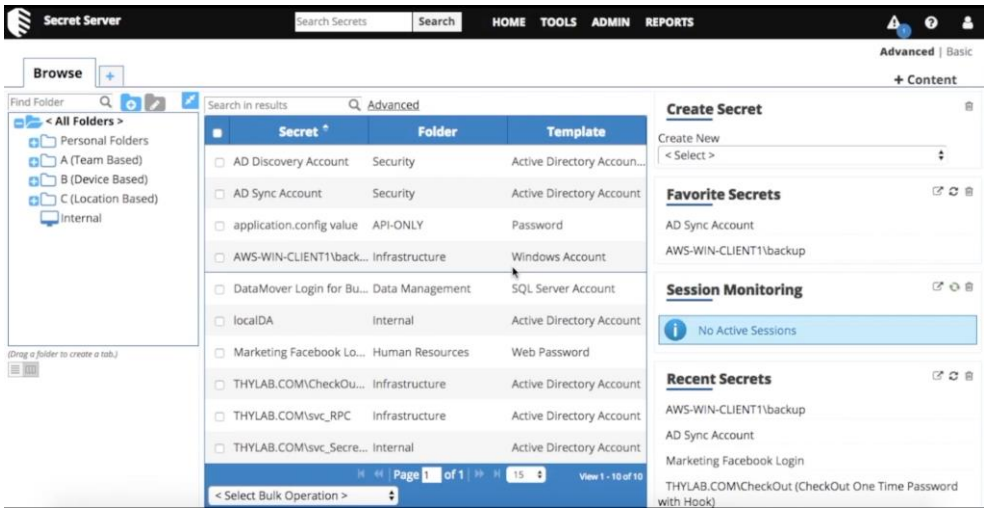

Рис. 3.1 Інтерфейс Verify Privilege Vault

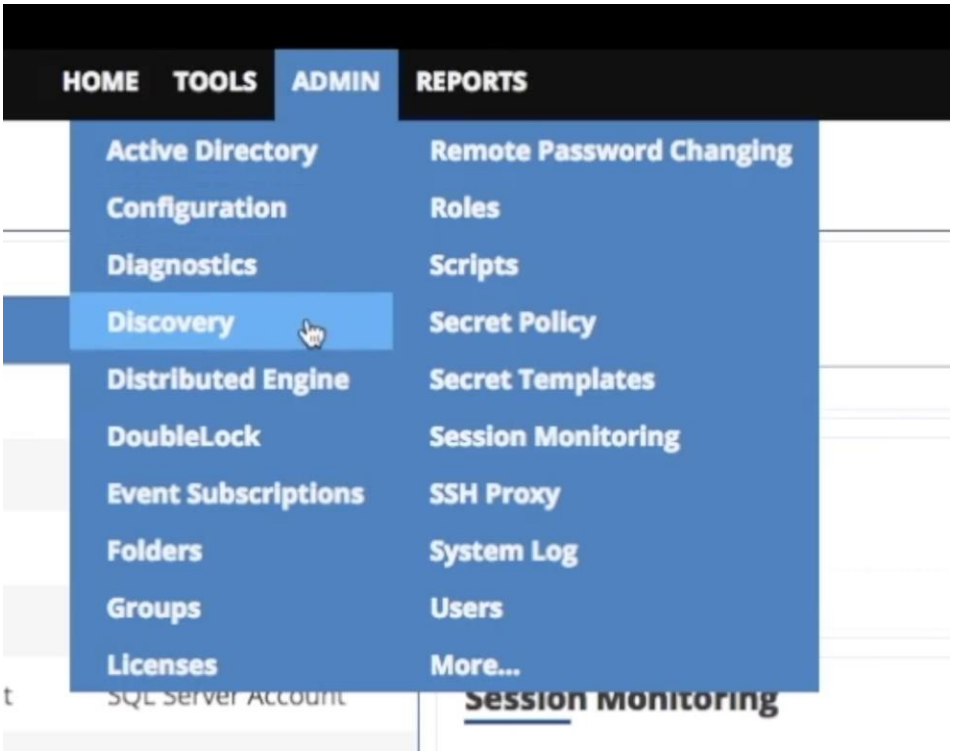

Рис. 3.2 Відкриття панелі «Discovery»
Verify Privilege Vault

Для перевірки мережі та пошуку необхідних акаунтів треба скористатися фукнцією Discovery Network View (рис. 3.3). За її допомогою Verify Privilege Vault шукає та відображає всі акаунти – локальні, сервісні та доменні (рис. 3.4) [11].

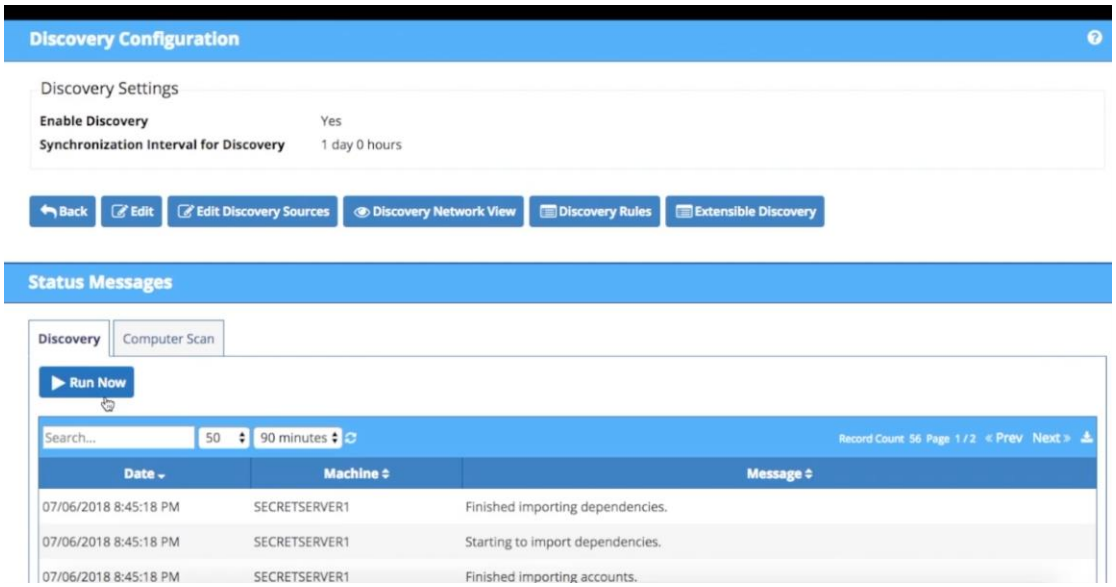

Рис. 3.3 Панель «Discovery»

Verify Privilege Vault

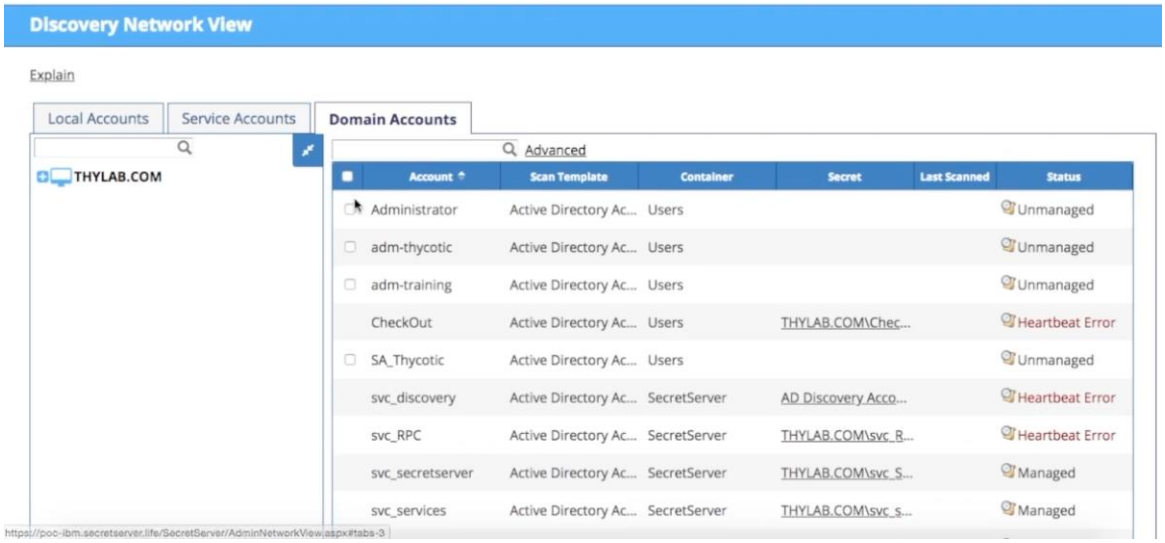

Рис. 3.4 Аналіз мережі та знаходження привілейованих аккаунтів

Verify Privilege Vault

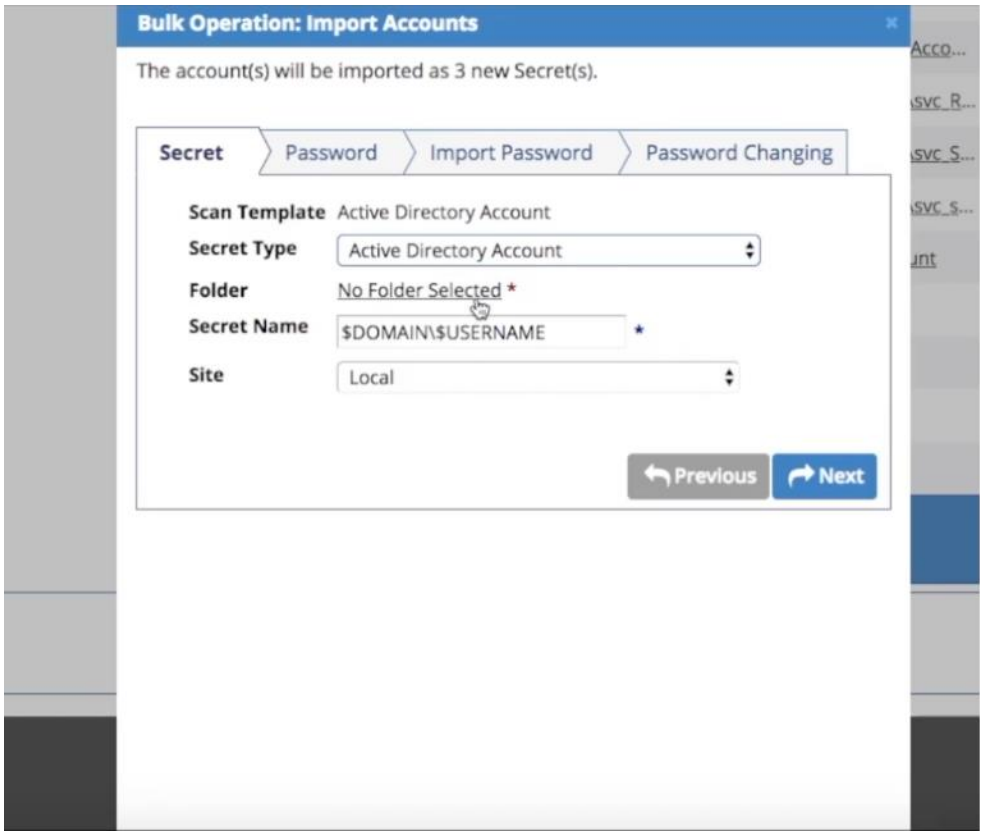

Рис. 3.5 Імпорт знайдених акаунтів у відповідну папку

Далі всі знайдені акаунти можна імпортувати у відповідних секрет та папку (рис. 3.5), а також визначити подалі дії щодо управління ними. Наприклад, змінити паролі після знаходження (рис. 3.6).

Також Verify Privilege Vault надає можливість автоматизувати ці дії. Для цього на панелі Discovery необхідно обрати функцію Discovery Rule та задати правило – за якими ключовими словами шукати користувача, які дії проводити після його знаходження та ін. (рис. 3.7) [11].

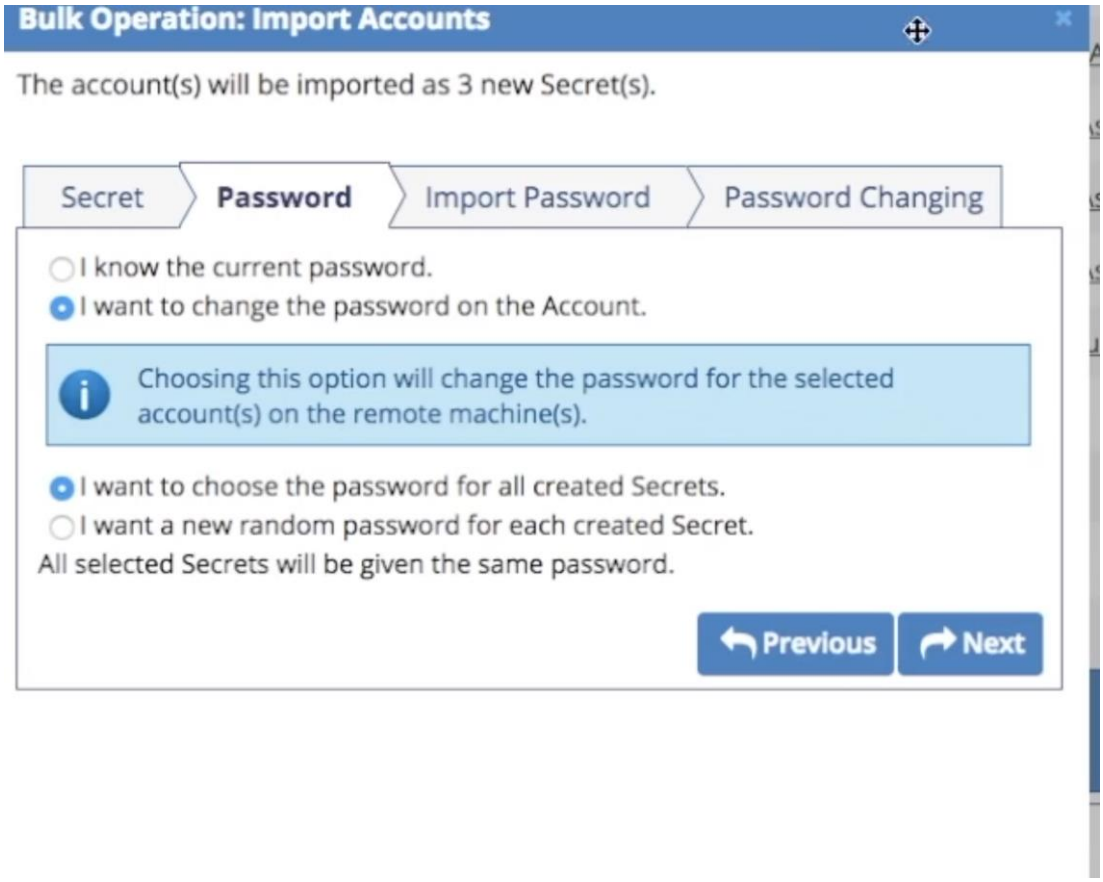

Рис. 3.6 Налагодження необхідних опцій по управлінню знайденими акаунтами

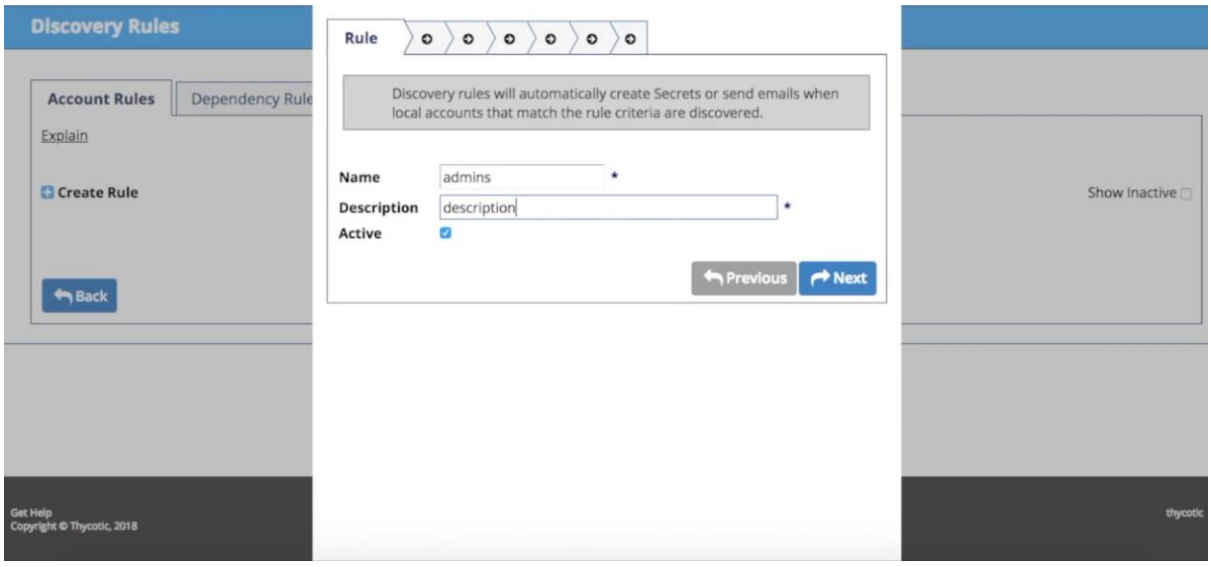

Рис. 3.7 Відкриття панелі «Discovery Rule»

Verify Privilege Vault

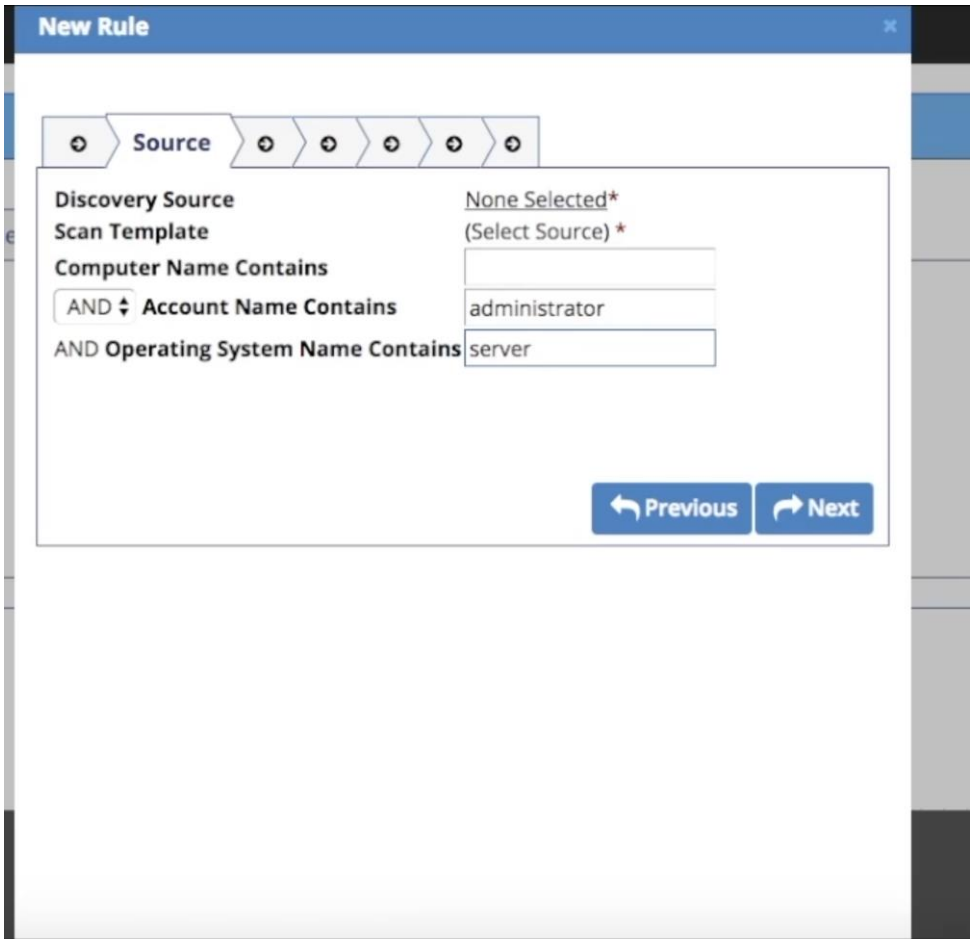

Рис. 3.8 Налаштування правила по управлінню знайденими привілейованими акаунтами

3.2.2 Захист привілейованих облікових записів та керування ними

Спільно використовувані привілейовані облікові дані, наприклад, облікові записи адміністратора, часто записуються на стікерах або заносяться у відкриті електронні таблиці. Але ці облікові дані дають доступ до найважливіших ресурсів організації.

За допомогою Verify Privilege Vault організації чітко побачать, які користувачі мають доступ до привілейованих облікових записів, яких саме, і як вони можуть користуватися цими правами доступу.

Програмний комплекс надає змогу контролювати акаунти, сортуя їх за папками (наприклад, по відділах організації) (рис. 3.9). Так, наприклад, всі облікові записи відділу маркетингу будуть мати доступ до відповідних даних [11].

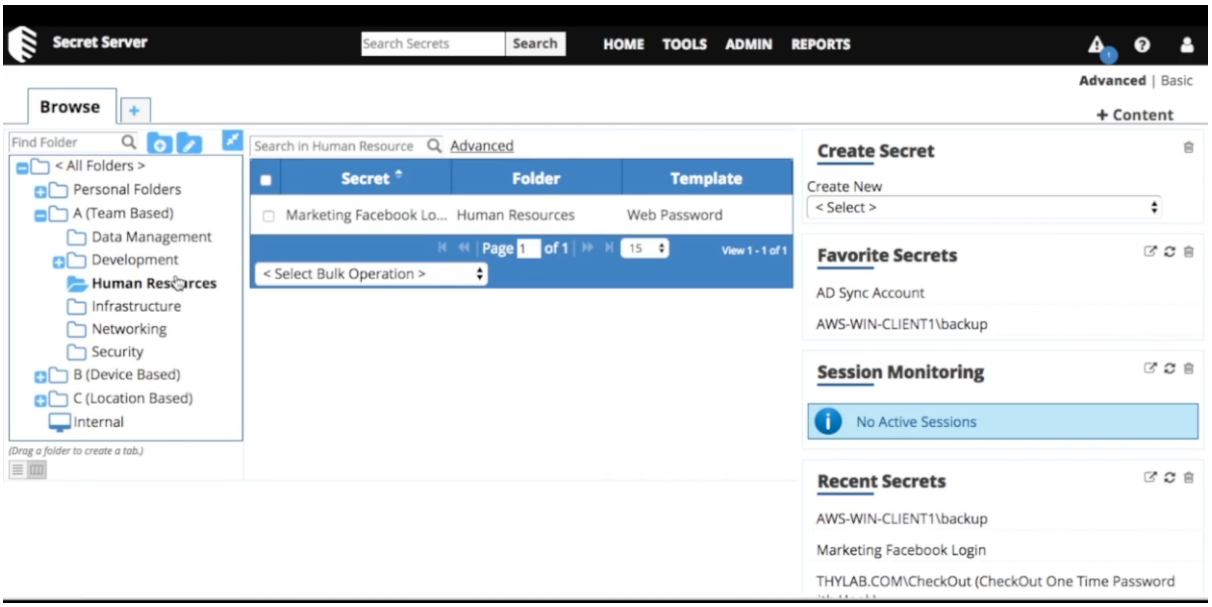

Рис. 3.9 Керування привілейованими обліковими записами

Також є можливість керувати доступом до даних окремих акаунтів. Наприклад, некритичним обліковим записам можна надали змогу копіювати та переглядати свій пароль (рис. 3.11).

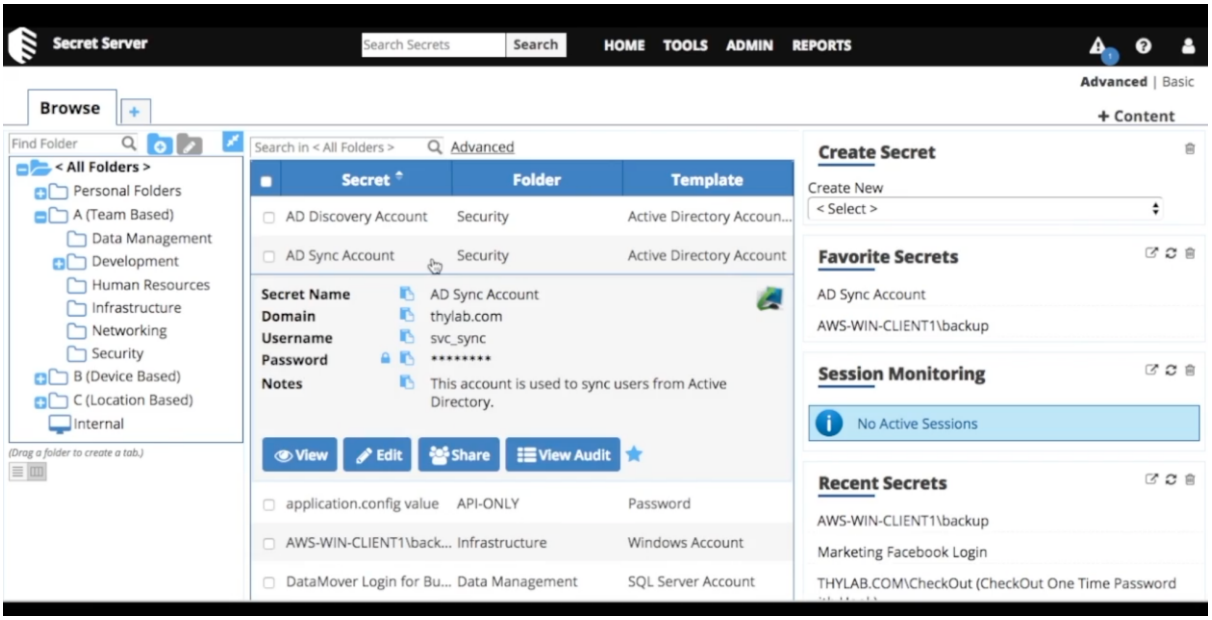

Рис. 3.10 Доступні для перегляду дані акаунта

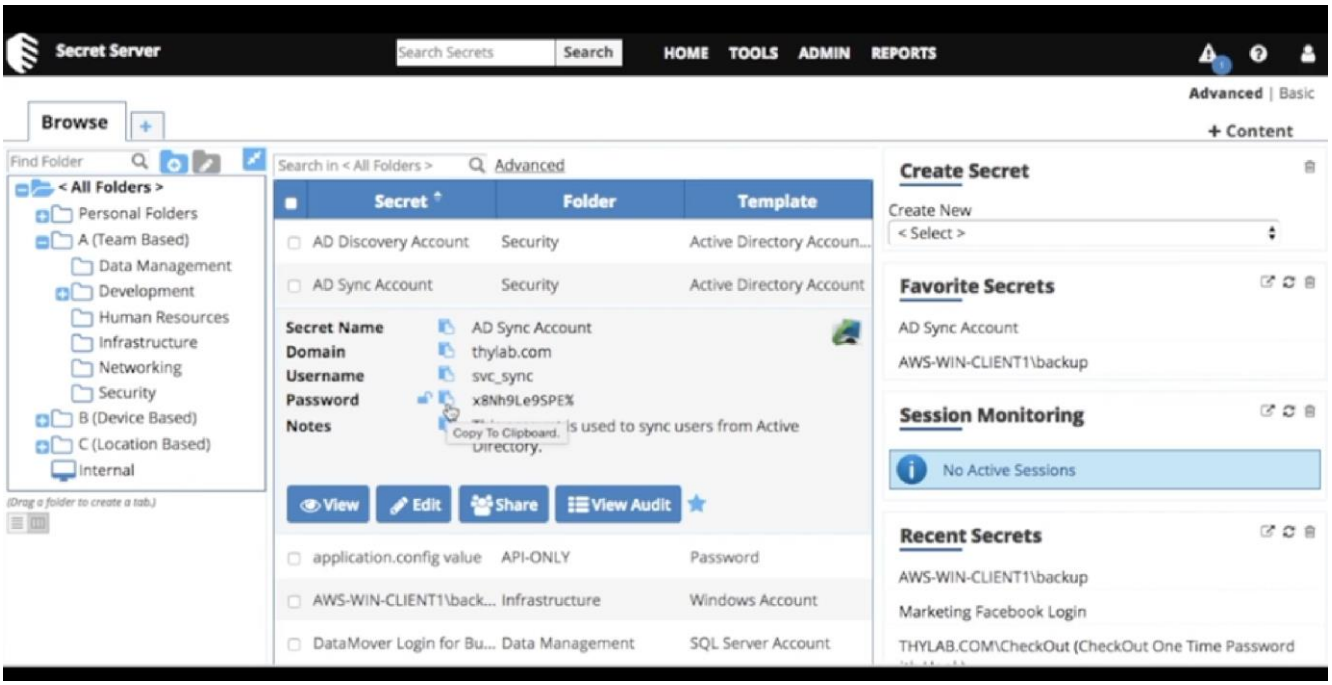

Рис. 3.11 Можливість перегляду паролю некритичного облікового запису

Для більш критичних облікових записів існує функція перегляду даних через Check Out – функція перевірки привілеїв у сховище (рис. 3.12).

Вона примушує несення відповідальності за секретні дані, надаючи ексклюзивний доступ одному користувачеві. Якщо секрет налаштовано для виведення, користувач може отримати до нього доступ. Якщо ввімкнена функцію «Змінити пароль під час реєстрації», після реєстрації Verify Privilege Vault автоматично примусово змінить пароль на віддаленому комп'ютері (рис. 3.13) [11]. Жоден інший користувач не може отримати доступ до секрету під час його виведення, за винятком необмежених адміністраторів. Це гарантує, що якщо доступ до віддаленої машини здійснюється за допомогою секретного коду, користувач, який його перевірив, був єдиним, хто мав належні облікові дані на той момент.

Для найкритичніших облікових записів та даних є можливість перегляду за запитом (рис. 3.15). Запит надсилається адміністратору, який на свій розсуд може надати доступ або не робити цього.

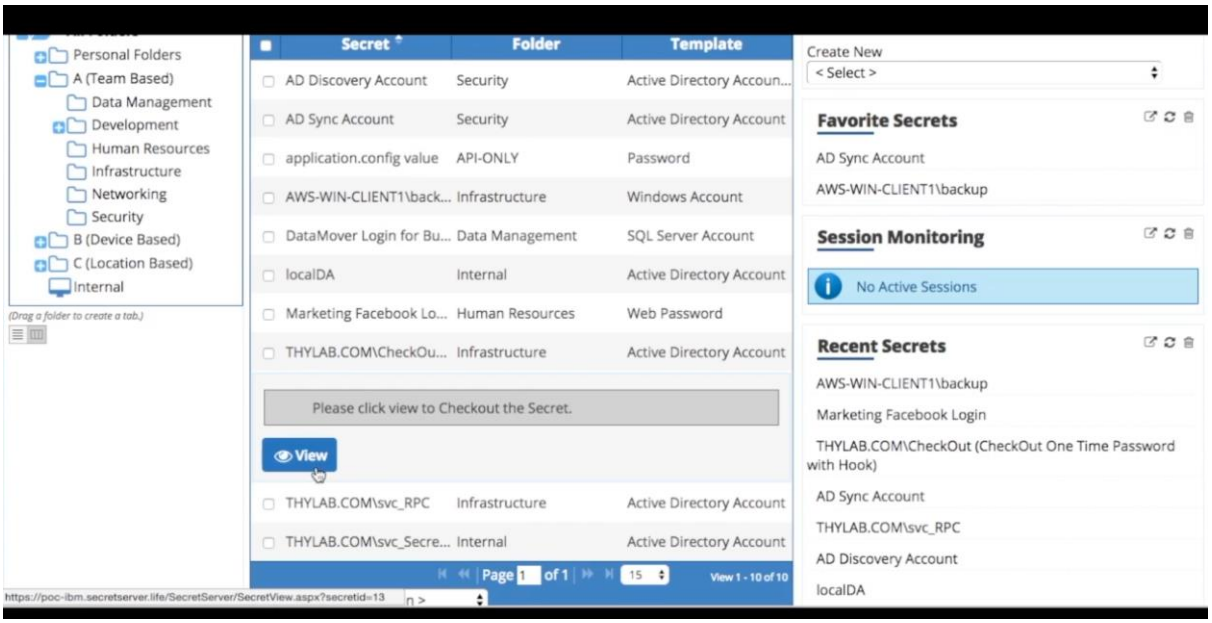

Рис. 3.12 Можливість перегляду паролю через Чек-аут

Рис. 3.13 Чек-аут

Також важливо зауважити, що кожна сесія моніториться та записується – адміністратор може переглянути, що робить користувач у любий момент та завершити його сесію примусово (рис. 3.14) [11].

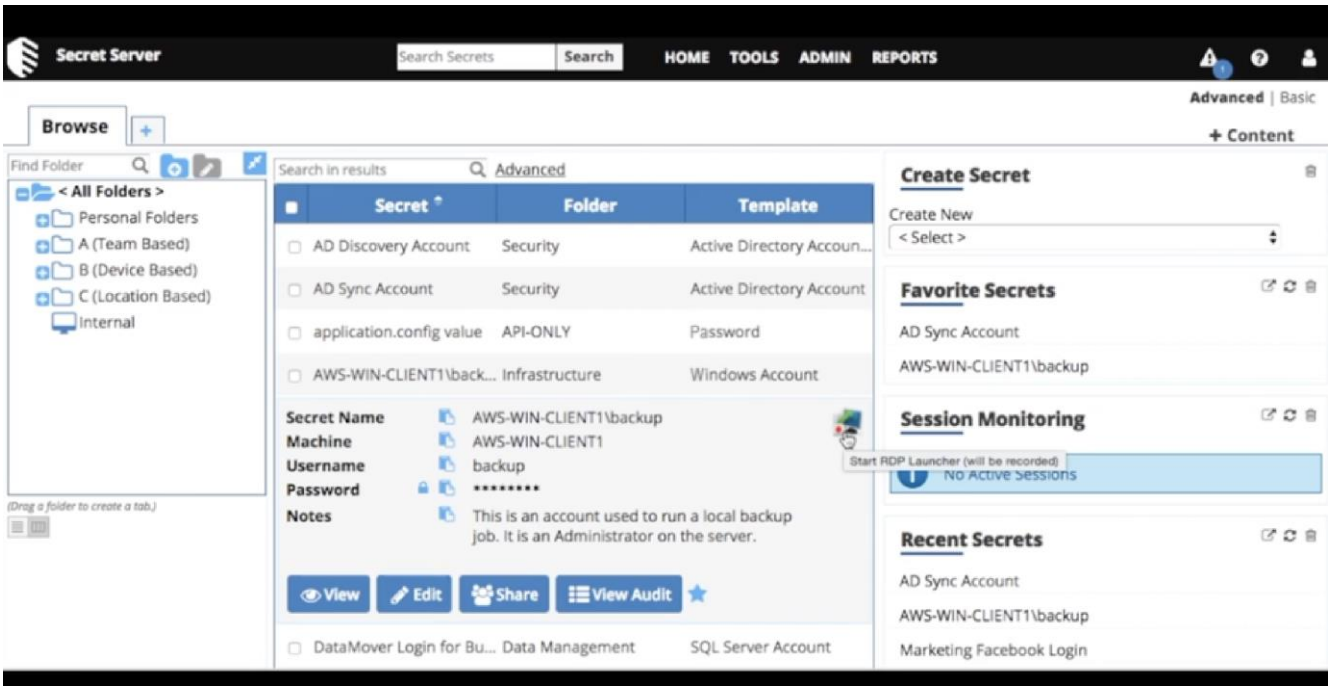

Рис. 3.14 Моніторинг сессії

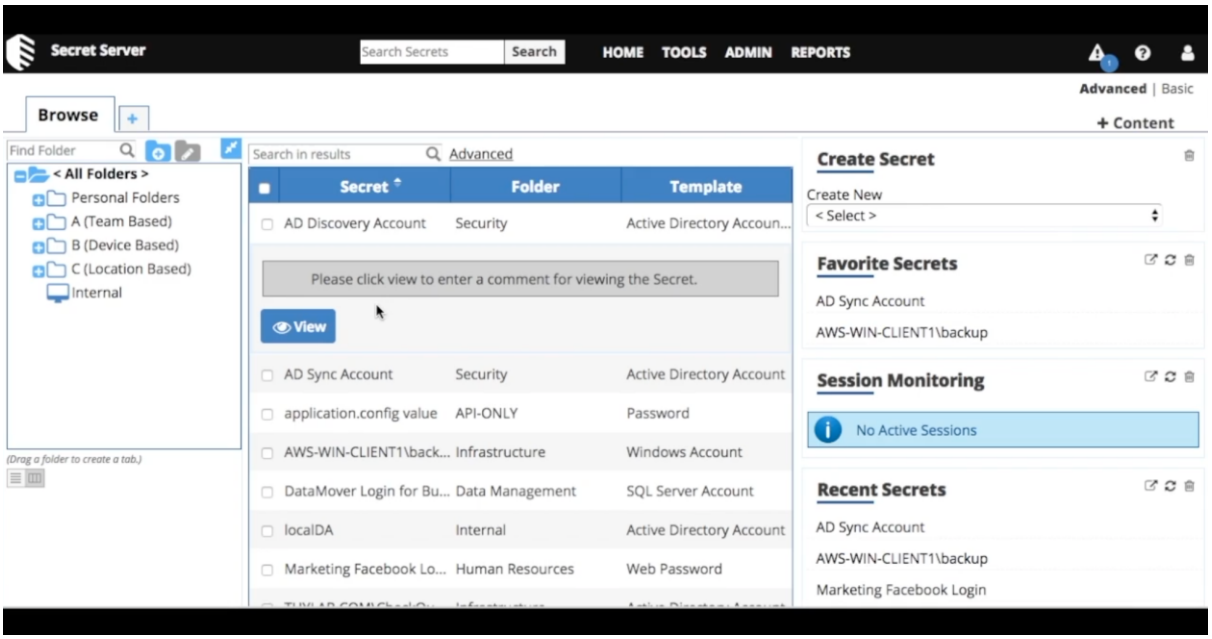

Рис. 3.15 Можливість перегляду даних облікового запису за запитом

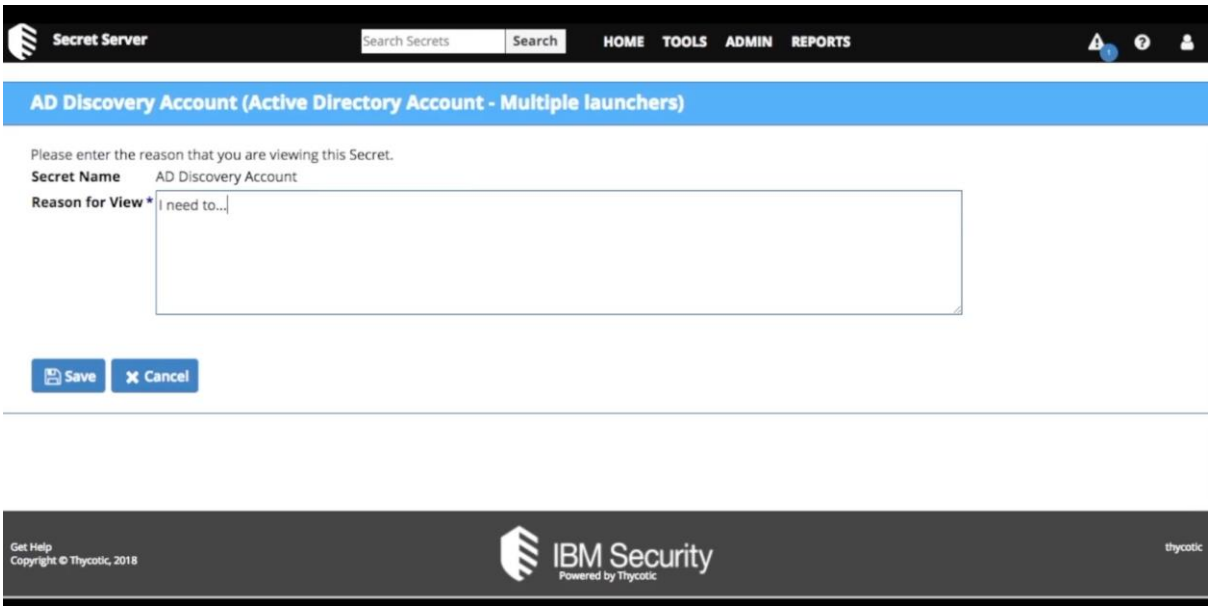

Рис. 3.16 Запит на перегляд даних

3.2.3 Відстеження привілейованих облікових записів

За наявності облікових записів, що використовуються спільно, часто складно розібратися, хто отримав доступ до систем і даних. Якщо хтось додає таємний обліковий запис, вносить несанкціоновану зміну або робить іншу ризиковану дію, то відстежити автора найчастіше неможливо.

За допомогою Verify Privilege Vault присутня можливість відстежувати та записувати сеанси привілейованого доступу, реєструючи кожне натискання клавіші. Це дозволить не лише повністю контролювати ці сеанси, а й прогнозувати наслідки.

Базовий запис сеансу є ліцензованою функцією в Verify Privilege Vault. Він покладається на обробник протоколу, налаштований на клієнтських машинах за допомогою програми запуску SS. За допомогою програми запуску Verify Privilege Vault робить посекундні знімки екрана на клієнтській машині під час записаного сеансу користувача. Ці зображення екрана користувача об’єднані у відео, яке можна завантажити та відтворити з метою аудиту та безпеки. Активність, записана під час сеансу, ґрунтується лише на змінах екрана.

Моніторинг сеансів дозволяє адміністраторам з дозволом на моніторинг сеансів переглядати всі активні запущені сеанси в Verify Privilege Vault. Якщо запис сеансу увімкнено за Секретом, адміністратор може спостерігати за сеансом користувача в режимі реального часу (рис. 3.20).

Також базовий набір функцій щодо моніторингу дозволяє адміністратору примусово завершити сесію на свій розсуд (рис. 3.19) [11].

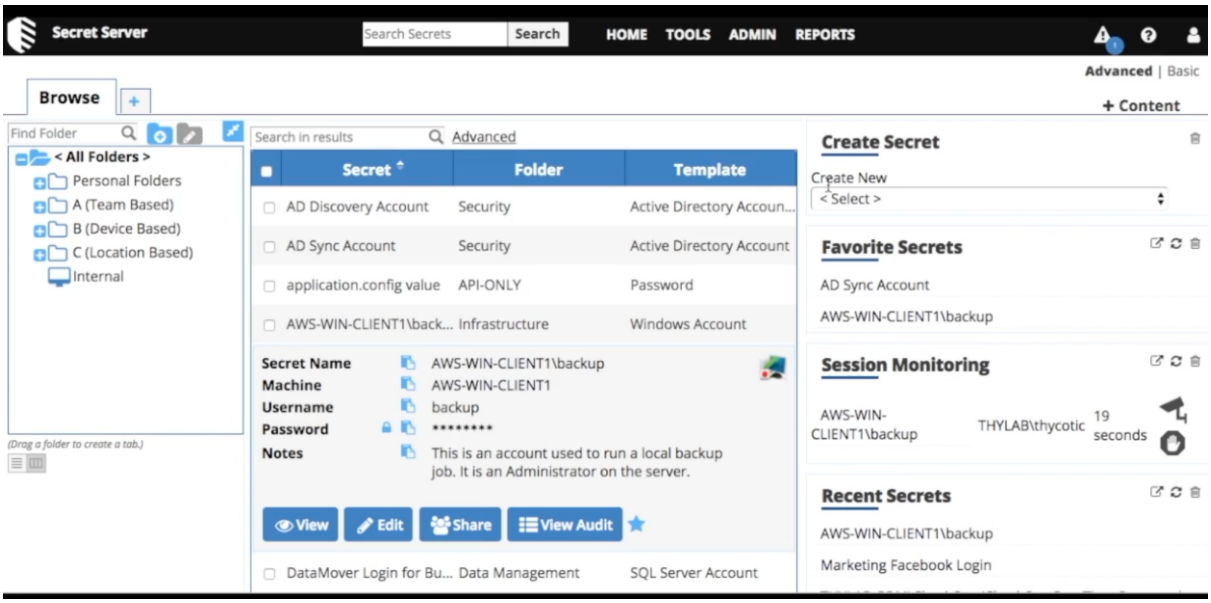

Рис. 3.17 Вибір сесії для моніторингу

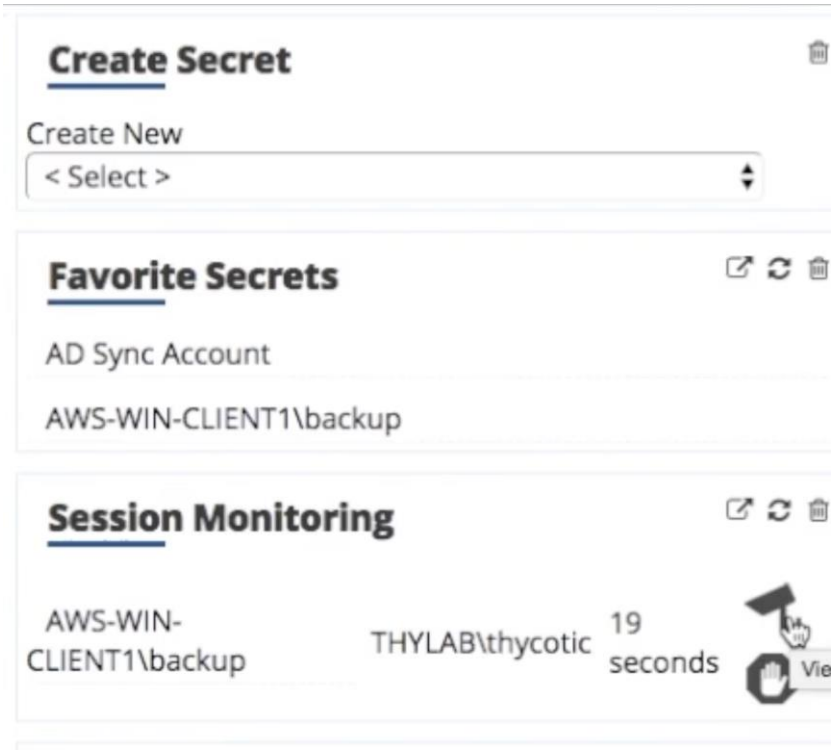

Рис. 3.18 Базові дані щодо моніторингу сесії

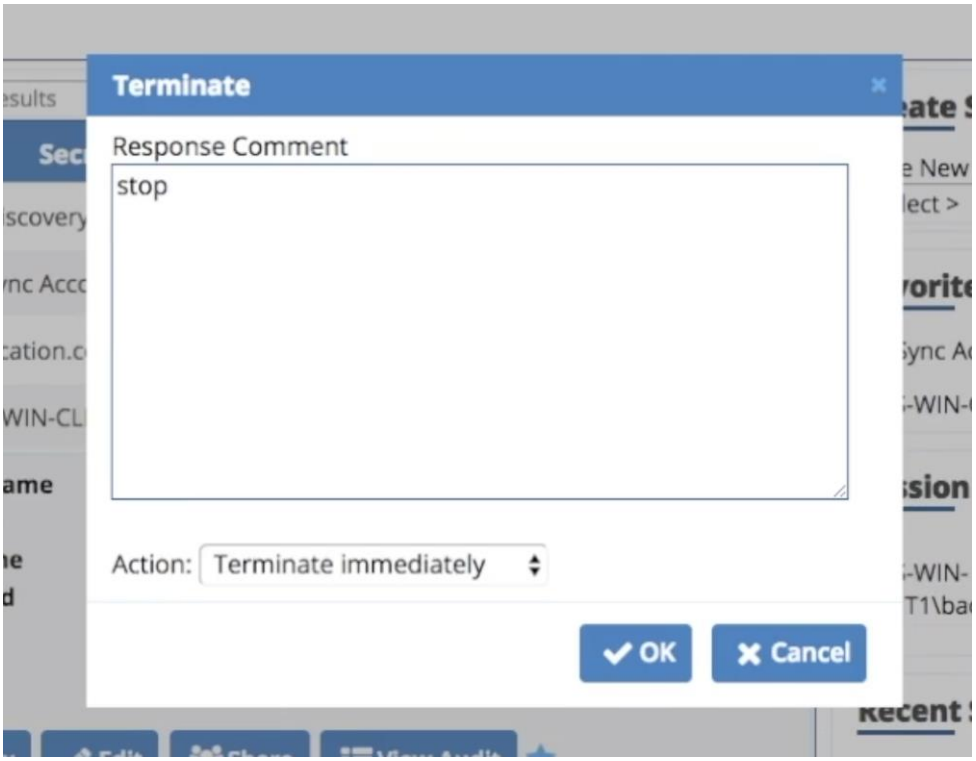

Рис. 3.19 Можливість примусового завершення сесії

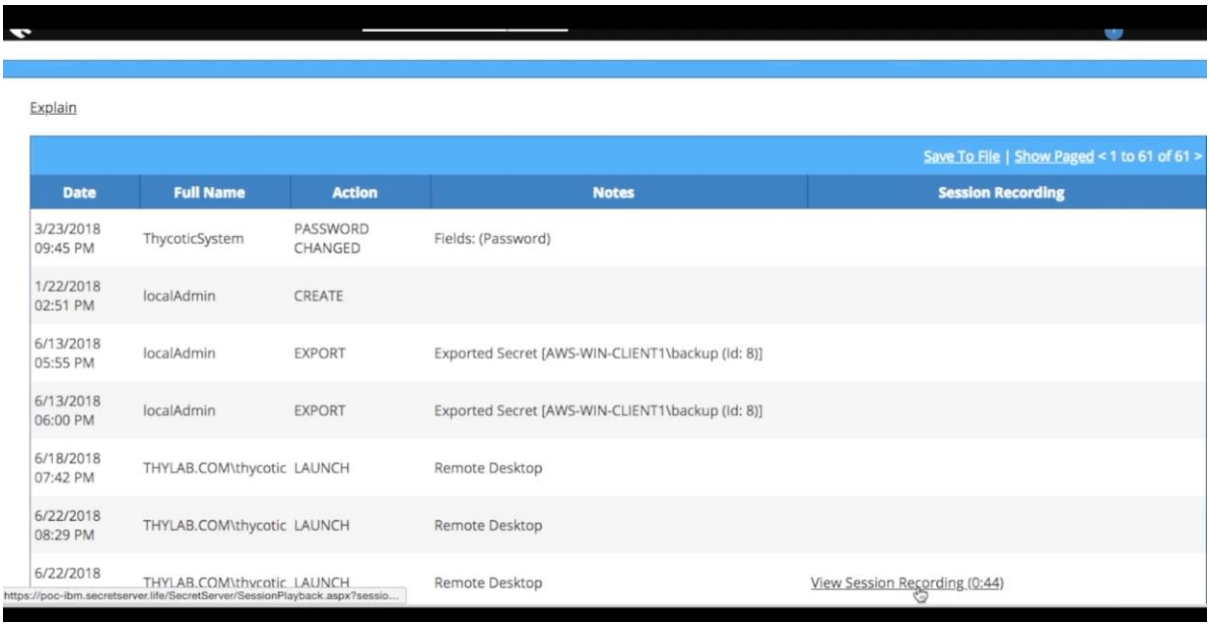

Рис. 3.20 Можливість перегляду сесії

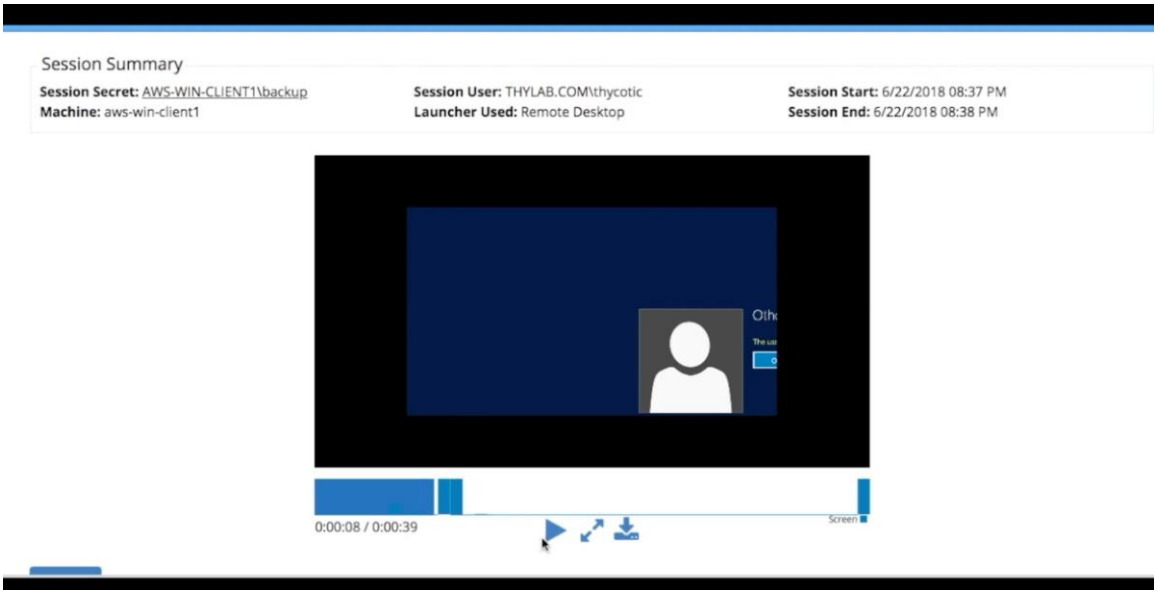

Рис. 3.20 Перегляд сесії в режимі реального часу

3.3 Розроблення рекомендацій щодо застосування технології управління привілейованим доступом в корпоративній інформаційній системі

Чим більш зрілі та цілісні політики безпеки та забезпечення привілеїв, тим краща можливість запобігати внутрішнім і зовнішнім загрозам і реагувати на них, а також відповідати вимогам.

Можна сформулювати наступні рекомендації щодо впровадження PAM в інформаційній системі організації:

1. Встановлення і запровадження всеосяжної політики управління привілеями: політика повинна регулювати те, як надаються/виключаються привілейований доступ та облікові записи; розглянути інвентаризацію та класифікацію привілейованих ідентифікаторів та рахунків; і застосовувати найкращі методи безпеки та управління.

2. Визначити та передати під керування всі привілейовані облікові записи та облікові дані: це має включати всі облікові записи користувачів та локальні; рахунки бази даних облікових записів додатків і служб; хмарні облікові записи та акаунти в соціальних мережах; ключі SSH; паролі за замовчуванням і жорстко закодовані; та інші привілейовані облікові дані, включаючи ті, які використовуються третіми сторонами/постачальниками. Discovery також має включати платформи (наприклад, Windows, Unix, Linux, Cloud, on-prem тощо), каталоги, апаратні пристрої, програми, служби/демони, брандмауери, маршрутизатори тощо [7].

Процес виявлення привілеїв має визначати, де і як використовуються привілейовані паролі, а також допомагати виявляти сліпі зони та зловживання безпеки, такі як:

- Покинуті облікові записи, які можуть надати зловмиснику бекдор до вашої критичної інфраструктури.
- Паролі без терміну дії.
- Неналежне використання привілейованих паролів, наприклад використання одного облікового запису адміністратора в кількох облікових записах служби.
- Ключі SSH повторно використовуються на кількох серверах.

3. Забезпечити мінімальні привілеї для кінцевих користувачів, кінцевих точок, облікових записів, програм, служб, систем тощо. Ключовою частиною

успішної реалізації найменших привілеїв є повне скасування привілеїв скрізь, де вони існують у вашому середовищі. Потім застосуйте технологію на основі правил, щоб підвищити привілеї, необхідні для виконання конкретних дій, анулюючи привілеї після завершення привілейованої дії [7].

Розбиті на тактичний рівень, найменше забезпечення привілеїв має охоплювати наступне:

- Вилучення права адміністратора на кінцевих точках. Замість надання привілеїв за замовчуванням для всіх користувачів за умовчанням треба надати стандартні привілеї, одночасно ввімкнувши підвищені привілеї для програм і виконання конкретних завдань. Якщо доступ спочатку не надано, але необхідний, користувач може надіслати запит до служби підтримки для схвалення. Майже всі (94%) уразливості системи Microsoft, розкриті у 2016 році, можна було б пом'якшити шляхом видалення прав адміністратора у кінцевих користувачів. Для більшості користувачів Windows і Mac немає підстав мати доступ адміністратора на своїй локальній машині. Крім того, коли справа доходить до цього, організації повинні мати можливість контролювати привілейований доступ для будь-якої кінцевої точки з IP-адресою — традиційного, мобільного, мережевого пристрою, IoT, SCADA тощо.
- Видалення усіх прав доступу root та адміністратора до серверів і зведіть кожного користувача до стандартного користувача. Це значно зменшить поверхню атаки та допоможе захистити ваші системи рівня 1 та інші критичні активи. Стандартні, «непривілейовані» облікові записи Unix і Linux не мають доступу до sudo, але все ще зберігають мінімальні привілеї за замовчуванням, що дозволяє виконувати базові налаштування та інсталювати програмне забезпечення. Звичайною практикою для стандартних облікових записів у Unix/Linux є використання команди sudo, яка дозволяє користувачеві тимчасово підвищити привілеї до рівня root, але без прямого доступу до облікового запису root і пароля. Однак, хоча

використання sudo краще, ніж надання прямого кореневого доступу, sudo створює багато обмежень щодо можливості перевірки, простоти керування та масштабованості. Тому організації краще обслуговуються, використовуючи технології керування привілеями серверів, які дозволяють детально підвищувати привілеї за потребою, забезпечуючи при цьому чіткі можливості аудиту та моніторингу.

- Застосування правил доступу з найменшими привілеями за допомогою контролю програм та інших стратегій і технологій, щоб видалити непотрібні привілеї з програм, процесів, Інтернету речей, інструментів (DevOps тощо) та інших активів. Застосовувати обмеження щодо встановлення програмного забезпечення, використання та зміни конфігурації ОС. Також обмежте команди, які можна вводити на дуже чутливих/критичних системах.
- Реалізування привілеїв, які також називаються привілеями «точно вчасно» (JIT): термін дії привілейованого доступу завжди закінчується. Підвищуйте привілеї за потребою для конкретних програм і завдань лише на той момент, коли вони потрібні.
- Обмеження доступ до привілейованого облікового запису якомога меншою кількістю людей.
- Мінімізування кількості прав для кожного привілейованого облікового запису [7].

4. Забезпечити поділ привілеїв та поділ обов'язків: заходи поділу привілеїв включають відокремлення функцій адміністративного облікового запису від стандартних вимог облікового запису, відокремлення можливостей аудиту/реєстрації в адміністративних облікових записах та відокремлення системних функцій (наприклад, читання, редагування, запис, виконання тощо).

Коли є найменші привілеї та поділ привілеїв, присутня можливість застосувати поділ обов’язків. Кожен привілейований обліковий запис повинен

мати привілеї, точно налаштовані для виконання лише окремого набору завдань, з невеликим перекриттям між різними обліковими записами.

При застосуванні цих засобів контролю безпеки, хоча IT-працівник може мати доступ до стандартного облікового запису користувача та кількох облікових записів адміністратора, він повинен бути обмежений використанням стандартного облікового запису для всіх рутинних обчислень і мати доступ лише до різних облікових записів адміністратора для виконання авторизованих завдань, які можна виконувати лише з підвищеними привілеями цих облікових записів [7].

5. Сегментування системи та мережі для широкого розділення користувачів і процесів на основі різних рівнів довіри, потреб і набору привілеїв. Системи та мережі, які вимагають більш високого рівня довіри, повинні впроваджувати більш надійні засоби контролю безпеки. Чим більше сегментація мереж і систем, тим легше запобігти поширенню будь-якого потенційного порушення за межі власного сегмента.

6. Застосування найкращих методів безпеки паролів:

– Централізувати безпеку й керування всіма обліковими даними (наприклад, паролі привілейованих облікових записів, ключі SSH, паролі програм тощо) у захищеному від несанкціонованого доступу сейфі. Запровадити робочий процес, згідно з яким привілейовані облікові дані можна отримати лише до завершення авторизованої дії, після чого пароль знову перевіряється, а привілейований доступ скасовується.
– Забезпечити надійні паролі, які можуть протистояти поширеним типам атак (наприклад, груба сила, на основі словника тощо), дотримуючись надійних параметрів створення паролів, таких як складність пароля, унікальність тощо.
– Регулярно змінювати паролі, зменшуючи інтервали зміни пропорційно чутливості пароля. Першочерговим пріоритетом має бути визначення та швидка зміна будь-яких облікових даних за замовчуванням, оскільки вони становлять величезний ризик. Для найбільш конфіденційного

привілейованого доступу та облікових записів запровадьте одноразові паролі (OTP), термін дії яких закінчується відразу після одноразового використання.

- Виключити обмін паролями — кожен обліковий запис повинен мати унікальний логін, щоб забезпечити чіткий контроль і чистий контрольний слід.
- Ніколи не розкривати паролі — застосуйте автентифікацію єдиного входу (SSO), щоб приховати паролі як від користувачів, так і від процесів.
- Видалити вбудовані/жорстко запрограмовані облікові дані та введення централізованого керування обліковими даними. Зазвичай для цього потрібне стороннє рішення для відокремлення пароля від коду та заміни його на API, який дозволяє отримати облікові дані з централізованого сейфа для паролів [7].

7. Відстежувати й перевіряти всі привілейовані дії: цього можна досягти за допомогою ідентифікаторів користувачів, а також аудиту та інших інструментів. Впроваджуйте керування та моніторинг привілейованих сеансів (PSM), щоб виявляти підозрілі дії та своєчасно ефективно досліджувати ризиковані привілейовані сеанси. Керування привілейованими сеансами включає моніторинг, запис і контроль привілейованих сеансів. Аудиторська діяльність повинна включати фіксацію натискань клавіш і екранів (що дозволяє переглядати в реальному часі та відтворювати). PSM має охоплювати період часу, протягом якого для облікового запису, служби чи процесу надаються підвищені привілеї/привілейований доступ.

Можливості PSM також необхідні для відповідності. SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA та інші нормативно-правові акти все частіше вимагають від організацій не тільки захищати та захищати дані, але й бути здатними довести ефективність цих заходів.

8. Застосовувати доступ з найменшими привілеями на основі вразливостей: застосовуйте дані про вразливості та загрози в реальному часі щодо користувача або активу, щоб уможливити динамічні рішення щодо доступу на основі ризиків. Наприклад, ця можливість надає функцію автоматичного обмеження привілеїв та запобігання небезпечним операціям, коли існує відома загроза або потенційна загроза для користувача, активу або системи [7].

9. Запровадити аналітику привілейованих загроз/користувачів. Встановіть базові показники для діяльності привілейованих користувачів і привілейованого доступу, а також відстежуйте й повідомляйте про будь-які відхилення, які відповідають визначеному порогу ризику. Також додайте інші дані про ризики для більш тривимірного уявлення про ризики привілеїв. Накопичення якомога більше даних не обов’язково є відповіддю. За умови присутності необхідних даних у формі, яка дозволяє приймати швидкі та точні рішення, щоб спрямувати вашу організацію до оптимальних результатів кібербезпеки.

Висновки до розділу 3

В даному розділі розглянуто та показано технології управління привілейованим доступом на базі програмного комплексу IBM Security Verify Privilege Vault. Розроблено варіант конфігурації програмного комплексу на основі документації розробника. Розглянуто особливості технології управління програмним комплексом. Розроблено загальні рекомендації щодо управління привілейованим доступом в сучасній корпоративній інформаційній системі.

ВИСНОВКИ

Метою даної роботи була розробка системи управління привілейованим доступом в сучасній корпоративній інформаційній системі на базі рішення IBM Security Verify Privilege Vault.

В роботі досліджено особливості та завдання управління привілейованим доступом та проаналізовані науково-технічні дані. В результаті було визначено головні проблеми управління привілейованим доступом у сучасних корпоративних інформаційних системах. Була встановлена необхідність управління привілейованим доступом для забезпечення кібербезпеки інформаційних систем.

Проаналізувавши наявні методи та засоби управління привілейованим доступом були встановлені критерії оцінки програмних комплексів щодо його реалізації.

Були визначені можливості програмного комплексу IBM Security Verify Privilege Vault та його основні архітектурні особливості щодо реалізації управління привілейованим доступом. Надані інструкції по базовій конфігурації для корпоративної інформаційної системи.

Проаналізовано можливості програмного комплексу IBM Security Verify Privilege Vault щодо виконання процесу управління привілейованим доступом у сучасному підприємстві.

Розроблено варіант конфігурації програмного комплексу для управління привілейованим доступом, а також показано технологію управління Security Verify Privilege Vault на прикладі найпоширеніших проблем щодо привілейованого доступу на сучасних підприємствах.

Розроблено загальні рекомендації щодо забезпечення якісного управління привілейованим доступом в корпоративній інформаційній системі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Информационные системы в экономике: Учебник / Под ред. В.В.Дика,- М.: Финансы и статистика, 1996 - 272 с.
2. Ахтырченко К. В., Леонтьев В. В. Распределенные объектные технологии информационных системах // СУБД.- 1997.- № 5-6.-С 52-64.
3. Павленко Л. А. Тексты лекций «Открытая информационна система», «Функциональные компоненты открытых распределых автоматизированных информационных систем» для студен¬тов специальности 7.080401 всех форм обучения.- Х.: Изд-во ХГЭУ, 2002.-52 с.
4. Айзенберг Э., Мелтон Д. Стандарты на практике // СУБД-1998.-№1-2.-С 102-110.
5. Козырев А. А. Информационные технологии в экономике и управлении: Учебник - СПб.: Изд-во Михайлова В. А., 2000.- 360 с
6. Павленко Л. А. Корпоративні інформаційні системи / Л. А. Павленко. – Харків: ІНЖЕК, 2002.
7. Privileged Access Management (PAM) [Електронний ресурс] // Beyond Trust. – 2021. – Режим доступу до ресурсу: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam.
8. Cannard M. Choosing the Right Privileged Access Management (PAM) Solution [Електронний ресурс] / Martin Cannard // Netwrix. – 2021. – Режим доступу до ресурсу: https://blog.netwrix.com/2021/10/06/privileged-access-management-solutions/.
9. Manage & Protect Privileged Accounts [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/security/digital-assets/iam/pam-from-ibm-wp/.

10. Verify Privilege Vault Documentation [Електронний ресурс] // 2021 – Режим доступу до ресурсу: https://ibm.docs.thycotic.com/isvp-vault/11.0.0.
11. IBM Security Verify Privilege Vault [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/ru-ru/products/verify-privilege-vault/details.
12. Resource Access Management [Електронний ресурс] // Cloud Native Toolkit. – 2021. – Режим доступу до ресурсу: https://cloudnativetoolkit.dev/resources/ibm-cloud/access-control/.
13. Guide to Role-Based Access Control (RBAC) [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/support/pages/guide-role-based-access-control-rbac.