ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

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

Виконав студент 6 курсу, групи БСЗМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Зеленко Є.Ю.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NIST - Національний інститут стандартів і технологій США

COBIT - Control Objectives for Information and Related Technology

PAM - Privileged Account Management

SRM- security and risk management

PASM - Privileged account and session managemen

PSM - Privileged session management

PEDM - Privilege elevation and delegation management

SM - Secrets management

SoD - Separation of Duties

СКПП — система контролю привілейованих користувачів

ВСТУП

Актуальність дослідження. Крадіжка привілейованих облікових записів використовувалася в більшості з найбільших кібератак. Організації постійно страждають від витончених забезпечених ресурсами кіберзлочинців, але існують заходи для зниження ризиків. Відносно прості поліпшення процесів і регламентів в поєднанні з технологіями управління привілейованим доступом, такими як управління сесіями і використання розширеної аналітики, можуть допомогти виявити скомпрометовані привілейовані облікові записи і зупинити зловмисників, перш ніж вони зможуть завдати шкоди організації.

Таким чино необхідно визначити методи та засоби захисту привілейованих даних інформаційної системи організації. Такі методи та засоби дозволять захистити привілейовані дані користувачів інформаційної системи організації. Вищенаведені аргументи актуалізують дослідження захисту привілейованих даних інформаційної системи організації.

Об’єкт дослідження – процес забезпечення захисту привілейованих даних інформаційної системи організації.

Предмет дослідження – технологія захисту привілейованих даних користувачів інформаційної системи організації

Мета роботи – розробити варіанти захисту привілейованих даних користувачів інформаційної системи організації та рекомендації щодо застосування технології їх захисту на підприємстві.

Наукові завдання:

захисту привілейованих даних користувачів інформаційної системи організації;

проаналізувати основні загрози використання привілейованих даних користувачів інформаційної системи організації;

проаналізувати методи та засоби захисту привілейованих даних користувачів інформаційної системи організації захисту привілейованих даних користувачів

інформаційної системи організації;

Розробити варіант технології захисту привілейованих даних користувачів інформаційної системи організації та розробити рекомендації фахівцям з кібербезпеки щодо застосування обраної технології.

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

Практичне значення одержаних результатів полягає в розробці варіанту налаштування основних модулів технології One Identity Safeguard захисту привілейованих даних користувачів інформаційної системи організації а також у розробці рекомендацій щодо використання даної технології в метою виявлення порушень з боку привілейованих даних користувачів інформаційної системи організації

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

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ДАНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1.Аналіз необхідності застосування привілейованого доступу інформаційної системи організації

Для захисту привілейованого захисту користувачів є багато рішень був затьмарений, які розширюють цінність певної технології на основі конкретних потреб організації. Зрештою, якщо кожне рішення проаналізувати, то кількість реалізованих рішень безпеки, починаючи від антивірусних та брандмауерів, закінчуючи моніторингом безпеки та рішеннями для єдиного входу, то знайдемо десятки постачальників та сотні окремих рішень у всій організації. Середній користувач або керівник не знає про більшість стеків технологій кібербезпеки, від яких вони залежать, навіть якщо вони можуть взаємодіяти з більшістю з них щодня.

Якщо згрупувати всі ці рішення на макрорівні, то виявимо що кожне з таких рішень потрапляє до однієї з трьох логічних груп. Це показано на Рис.1.1.

Ці логічні групи можна охарактеризувати як

• Ідентифікація - Захист ідентичності користувача, облікового запису та облікових даних від неналежного доступу

• Привілеї- захист прав, привілеїв та контролю доступу для особи або облікового запису

• Актив - захист ресурсу, що використовується особою безпосередньо або як послуга

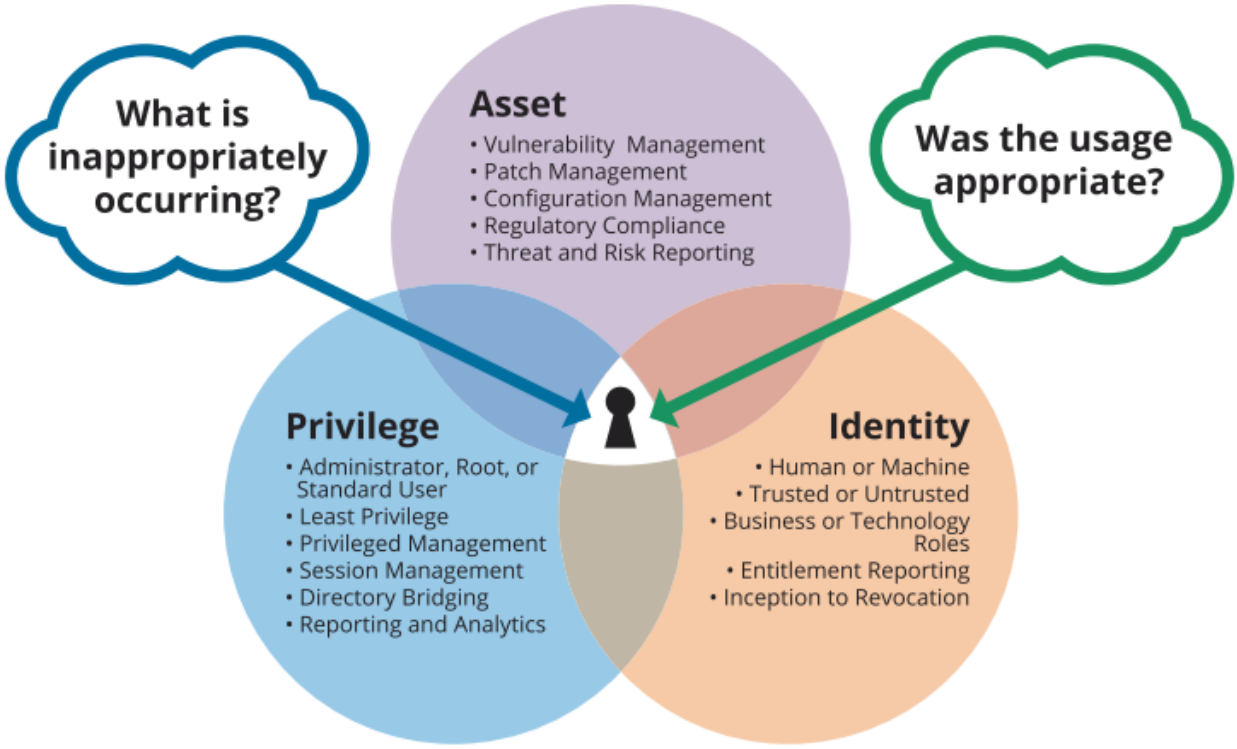


Рис.1.1. Логічні групи рішень доступу до ІС

Існує багато фреймворків, які допомагають організаціям визначити, організувати, реалізувати та покращити кібербезпеку їх інформаційних систем. Такі фреймоворки з кібербезпеки представляють Control Objectives for Information and Related Technology (COBIT), Національний інститут стандартів і технологій США (NIST), Міжнародна організація стандартизації (ISO) - усі вони надають основи для орієнтації на мислення програм кібербезпеки. Вони є основою, оскільки вони дають детальні вказівки з усього, починаючи від фінансування та закінчуючи готовністю реагувати на інциденти безпеки.

Однією з найбільших проблем, з якими стикаються всі фреймворки кібербезпеки безпеки, є їх складність.

Управління ідентифікацією є частиною більшості, якщо не всіх, «офіційних» систем безпеки. Тож розглянемо п’ять А для забезпечення управлінням кібербезпекою. На рис.2.1 показано опис цієї концепції. В цій концепції пропонується скорочене

визначення та можливості того, як можна представити управління ідентифікацією як набір універсальних принципів, які застосовуються до всіх встановлених систем безпеки та майже до всіх сценаріїв безпеки підприємства. Концепція “П’ять А” - це автентифікація, авторизація, адміністрування, аудит та аналітика. Як тільки буде забезпечена дана концепція, то буду можливість встановити контроль управління ідентифікацією практично за будь -яким сценарієм для будь -якого типу організації чи вертикальної галузі.

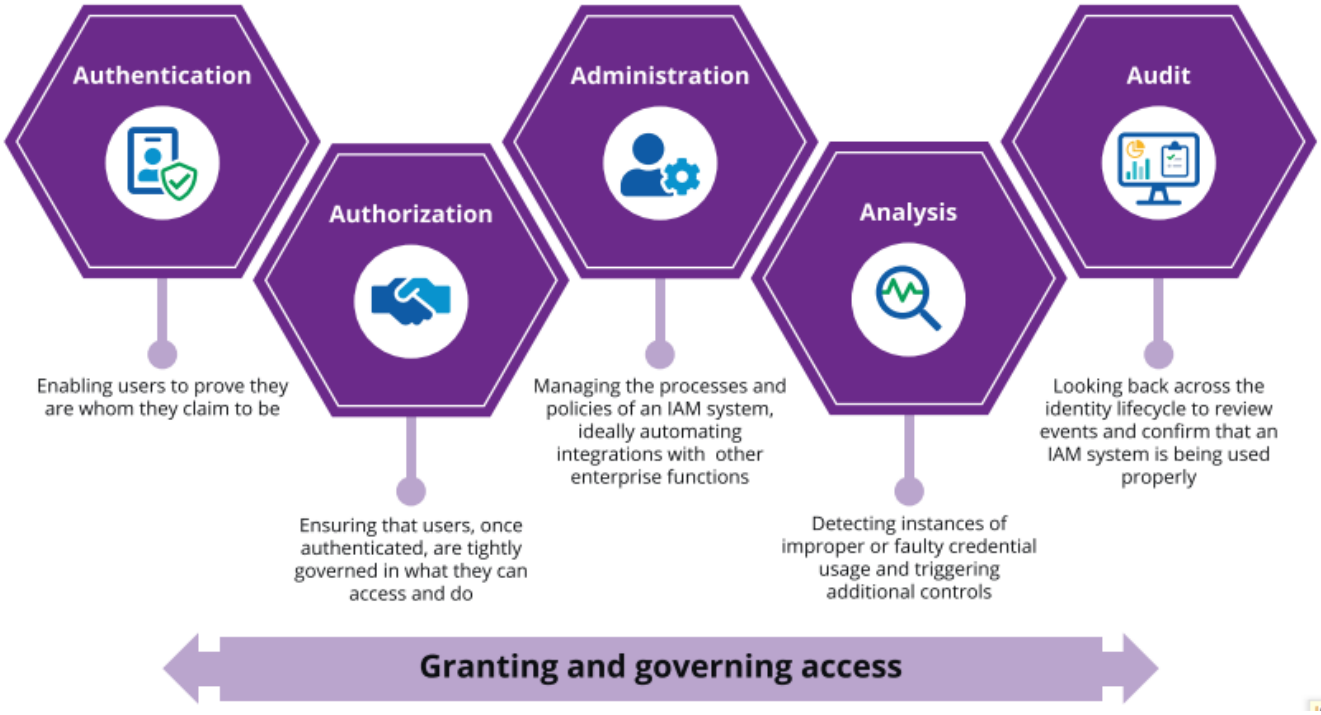


Рис. 1.2. П’ять А для забезпечення управлінням кібербезпекою

Аутентифікацію часто плутають з авторизацією, навіть якщо це різні технології та практика. У деяких інформаційних системах автентифікація та авторизація змішуються між собою і не розрізняються або не розмежуються у впровадженні чи управлінні. Наприклад, Apple iOS використовує біометричні дані як для авторизації, так і для автентифікації, а взаємодія з кінцевим користувачем розмивається незалежно від типу дії.

Тож надаймо визначення, автентифікація - це логін (ім’я користувача) на додаток до певної форми секрету, історично отриманого пароля, для встановлення доказу чи довіри до особи. По суті, це підтвердження того, ким ви себе називаєте.

Автентифікація вашої особи = логін + спільний секрет (пароль)

Хоча існує багато варіантів спільних секретів, які можна використовувати для входу, таких як пін-коди, паролі, ключі, двофакторна автентифікація тощо, сам логін, як правило, не є таємницею і його часто можна вгадати для ідентичності. Наприклад, логін може бути "zelenko" для мого псевдоніма як абревіатура призвища Зеленко. Однак логін також може бути чимось більш складним, наприклад номер співробітника, який краще маскує ідентичність користувача. Для високозахищених середовищ цей другий підхід є кращим, особливо згідно рис. 2.1 для облікових записів адміністратора або root. Ви не можете візуально ідентифікувати привілеї з обліковим записом, просто переглядаючи обліковий запис або ім’я користувача. Невідомість - це не безпека, але вона часто допомагає! Отже, простими словами, автентифікація - це не що інше, як доведення вашої особи або власності на певний обліковий запис. Він не надає дозволів, привілеїв або доступу, а лише підтвердження того, що ви є тим, ким ви себе називаєте.

Авторизація - це наступний шаг після автентифікації. Користувач не можете бути авторизованими для виконання функцій, мати визначені привілеї або навіть виконувати завдання у цих ролях без попередньої аутентифікації. Якщо адміністратор надає гостьовий пакет у додатках або операційній системі і у користувача немає власного логіну та / або пароля, автентифікація вважається гостьовою, а ви надаєте всі права та привілеї цьому гостю. Тож користувач пройшов аутентифікацію та отримав авторизацію, хоча і дуже невелику.

Авторизація = привілегії (що вам надано) + аутентифікація

Таким чином, авторизація - це право виконувати функцію, засновану на вашій аутентифікації. Ваша особистість та пов'язаний з нею обліковий запис надають привілеї для виконання певних функцій, а також може бути явно відмовлено або не врегульовано виконання інших функцій. Ці привілеї можуть бути призначені в додатках, операційній системі або в якій-небудь частині, що підтримує інфраструктуру. Привілеї також можуть бути призначені у системі управління ідентифікацією або привілеями, які його контролюють. Для масштабного управління завжди рекомендується остання.

Коли одинакові привілеї згрупувалися разом, вони створювали основу для визначення ролі. Коли Роль визначає групи облікових записів, Роль забезпечує повноту цієї групи для виконання цих функцій.

Під адміністрацію будемо розуміти контроль автентифікації, авторизації та аудиту. Адміністрація означає управління конфігурацією та контроль за будь -якими змінами, внесеними до автентифікації, авторизації та аудиту.

Аудит. Сприяючи забезпеченню повторюваного та сталого доступу користувачів, процес аудиту також є обов’язковим процесом управління ідентичністю. Незалежно від того, чи є це використання спеціальних засобів управління для дотримання нормативних вимог, або створення функцій управління життєвим циклом, керованих системою, які є стабільними та перевіряються як доказ контролю, аудит є важливою частиною системи управління ідентифікаційними даними.

Для деяких аудит IAM означає надання програми сертифікації доступу користувачів. Для інших це визначення та впровадження превентивної та детективної політики, такої як розподіл обов’язків.

П'ятий і останній А - це комплексний аналіз того, як працює система IAM. Аналітика означає отримання оперативної інформації та інформації про безпеку шляхом постійного збору та обробки даних щодо конфігурації, призначення та

використання даних, що стосуються ідентичності. Розширена аналітика ідентичності дозволяє більш поінформований та передбачувальний підхід до управління. Використовуючи методи машинного навчання (ML) та штучного інтелекту (AI), інструменти аналізу ідентичності можуть надавати важливу інформацію аналізу групи записів, яка допомагає розширити функції аудиту і адміністрування ідентичності та зробити їх більш динамічними та чуйними. Наприклад, якщо аналітичний механізм виявляє підозрілий, недоречний або незвичайний доступ, він може запропонувати адміністраторам переглянути цей доступ, щоб переконатися, що була реалізована правильна конфігурація. Аналітика може надавати автоматично створені аналітичні дані та рекомендації, які дозволяють галузі бізнесу приймати більш обґрунтовані рішення щодо доступу, які підвищують безпеку та забезпечують відповідність. Завдяки досягненням у сфері машинного навчання та штучного інтелекту, тепер можна виявляти та обробляти великі кількості отриманих даних, щоб виявити приховані загрози, що виходять далеко за межі того, чого можна досягти завдяки правилам.

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

Відповідно до вищесказаного в організаціях необхідно застосовувати управління привілейованим доступом (Privileged Account Management, PAM) [2]. Застосування такої технології надає ряд перева, а саме:

зменшити площу атаки;

пом'якшити вплив кібератаки на інформаційну систему,

підвищити продуктивність роботи для аналітики,

знизити ризик від помилок користувача при роботі з інформаційною системою.

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

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

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

Привілеї включають в себе дозволи на виконання таких дій:

вимикання систем;

завантаження драйверів пристроїв;

настройка мереж або систем;

підготовка і настройка облікових записів користувачів, додатків тощо;

підготовка і настройка хмарного доступу і т. п.

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

Наведемо приклад привілейованого доступу користувачів інформаційної системи [2] рис 1.3.

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

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

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

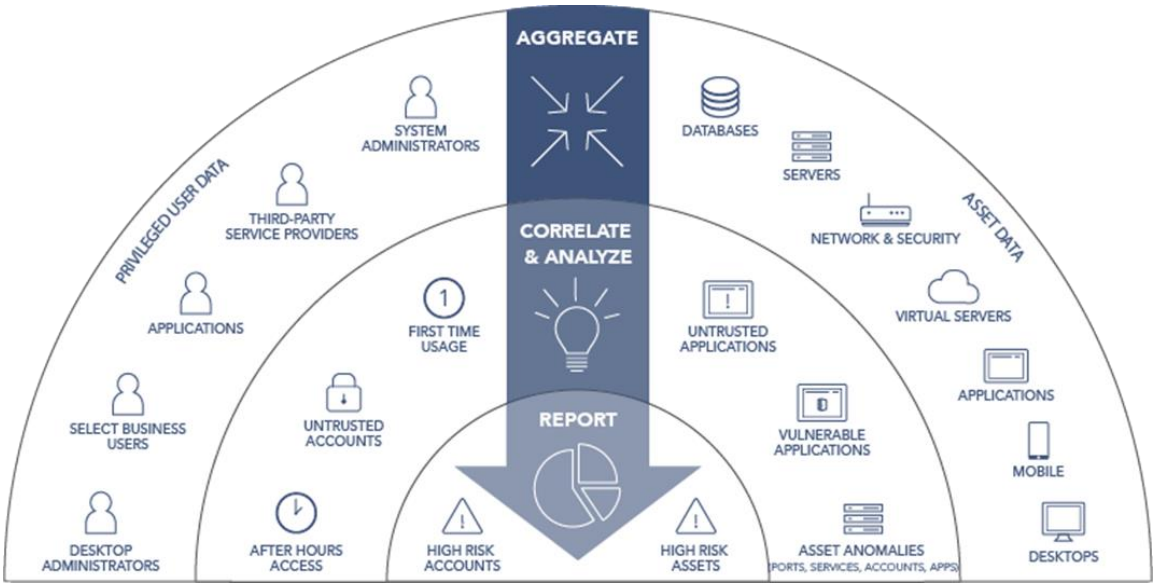


Рис.1.3. Користувачі привілейованого доступу

Сервісні акаунти - привілейовані локальні або доменні облікові записи, які використовуються додатком або службою для взаємодії з операційною системою.

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

Рис. 1.4. Привілейований доступ

Привілеї дозволяють користувачам, додаткам і іншим системним процесам права доступу до певних ресурсів. У той же час можливість зловживання з боку як внутрішніх, так і зовнішніх зловмисників створює для організацій серйозну загрозу безпеці.

Зовнішні та внутрішні загрози привілейованих доступів – це хакери, шкідливі програми, партнери, інсайдери, призначені для користувача помилки є найбільш поширені вектори привілейованих загроз.

Переваги управління привілейованим доступом:

Чим більше привілеїв і доступу до користувача, облікового запису або процесу накопичується, тим більша ймовірність зловживання, експлойта або помилки. Реалізація управління привілеями не тільки мінімізує ймовірність виникнення порушення безпеки, але також обмежить область порушення в разі його виникнення.

PAM може демонтувати кілька точок ланцюжка кібератак, забезпечуючи захист як від зовнішніх атак, так і від внутрішніх атак, які можуть відбутися в мережах.

Обмеження привілеїв для людей, процесів та програм зменшить площу атаки, захищаючи від зовнішніх і внутрішніх загроз.

З PAM зменшиться поширення шкідливих програм, адже багато їх різновиди потребують підвищених привілеї для установки або запуску. Видалення надмірних привілеїв, таких як примусове застосування найменших привілеїв в масштабах підприємства, завадить шкідливому ПО закріпитися в системі.

Знизиться ймовірність виникнення проблем несумісності між додатками або системами і сам ризик простоїв.

Управління привілейованим доступом допоможе створити менш складну і, отже, більш просту для аудиту середовище.

Рис.1.5. Робочий процес привілейованого управління паролями

1.3. Загрози та міри захисту привілейованого доступу

Розглянемо питання загроз привілейованому доступу. Атаки на привілейованих користувачів, таких як системні адміністратори, трапляються, але набагато частіше зловмисники вибирають більш просту початкову мету. Звичайні співробітники, як правило, менш технічно підковані, і їх простіше атакувати. Як тільки облікові дані користувача скомпрометовані, зловмисники перемикають увагу на кінцеву мету - привілейовані облікові записи.

Більшість атак починаються з спроби обдурити нічого не підозрюючих користувачів. В ході фішинговою атаки зловмисник за допомогою пошти, месенджерів або соціальних мереж намагається переконати жертву поділитися цінною інформацією (такою як облікові дані), а також пропонує відкрити документ,

або перейти по посиланню, в результаті чого встановити шкідливе ПЗ на комп'ютер користувача.

Як тільки зловмисники потрапляють в IT-середовище жертви, починається стадія внутрішньої розвідки. Вони спробують зібрати якомога більше інформації про інфраструктуру, скласти карту мережі і систем. Знання мережі допомагає хакерам отримати більш високі привілеї і досягти кінцевої мети - наприклад, отримати доступ до контролера домену. Передача хеша (Pass-the-hash), перехоплення SSH-ключа, експлойти ядра і служб - три основні методи, які використовуються для підвищення привілеїв. Це дозволяє встановити практично повноцінний контроль над цільовою системою [4]. На рис.1.6 показано вектор атаки отримання привілейованого доступу.

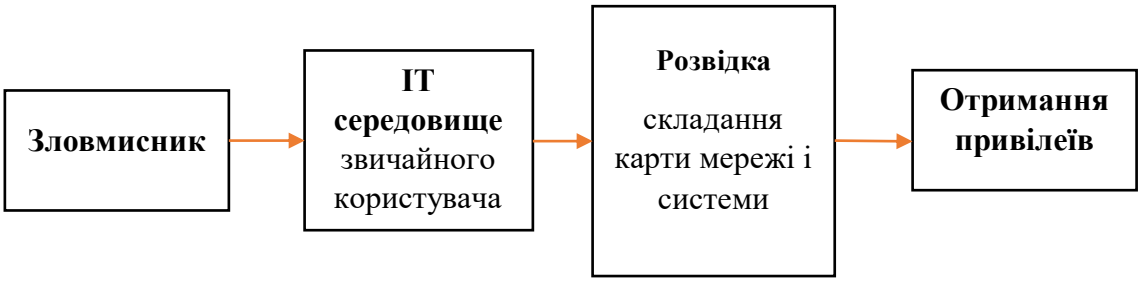


Рис.1.6. Приклад атаки отримання привілейованого доступу

Тож розглянемо міри захисту привілейованого доступу.

Аудит і посилення організаційних заходів безпеки є одним з простих і ефективних способів знизити ризик крадіжки привілейованих облікових записів [4].

Це можна зробити сформувавши повний і актуальний список привілейованих облікових записів.

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

Основні міри захисту привілейованого доступу:

1. Обмежити область дії кожного привілейованого облікового запису.

Для цього необхідно використовувати принцип найменших повноважень для всіх привілейованих облікових записів: кожен обліковий запис повинен мати тільки ті права, які необхідні для виконання конкретного завдання. Наприклад, обліковий запис для адміністрування програми не повинен мати ніяких системних привілеїв, крім необхідних для внесення змін в конфігурацію програми та його перезапуску. Заводити облікові записи тільки в тих системах, де вони потрібні [4].

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

Переміщення та звільнення співробітників часто зазвичай викликають проблеми з безпекою, які пов'язані з наявністю прав, яких не повинно бути у співробітників. У випадку з зовнішніми підрядниками управління ситуацією ще більш складне, особливо коли доступ необхідно зробити тільки для короткострокового проекту [4].

3. Формалізувати політику паролів

Компанії з високим рівнем безпеки зазвичай застосовують формалізовану політику паролів для привілейованих облікових записів. Крім стандартних вимог, характерних для всіх облікових записів, слід заборонити або посилити контроль за спільним використанням привілейованих облікових записів [4].

4. Впровадження технологій для контролю привілейованого доступу управління паролями

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

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

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

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

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

Тож необхідно впровадити управління сесіями.

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

Централізоване управління політиками, які дозволяють обмежити активність користувачів.

Моніторинг дій привілейованих користувачів в режимі реального часу.

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

Подвійний контроль з авторизацією супервайзера для роботи в особливо критичних системах.

Оповіщення та розрив сесій в разі порушення політик.

Тож управління сесіями знижує ризик злому або несанкціонованого доступу до важливих активів IT системи організації, обмежуючи типи активів, до яких можна отримати доступ, і типи команд, які можуть бути виконані. Однак, це не дозволяє оперативно виявляти факти компрометації облікових записів. У цьому допомагають технології машинного навчання і аналітики [4].

5. Аналітика поведінки користувачів для контролю привілейованого доступу

Цільові атаки часто використовують інструменти нульового дня для реалізації сценаріїв атак. Традиційні рішення по ІБ, такі як SIEM, часто не справляються із завданням виявлення, так як використовують методи детектування, засновані на правилах. Багато типів атак залишаються непоміченими. Саме цю проблему закриває аналітика поведінки користувачів.

Біологи визначають поведінку будь-яких живих організмів як скоординовані реакції на внутрішні і / або зовнішні подразники, тому поведінка - це все, що ми робимо свідомо. Точно так же цифрове поведінка - це всі, наші дії в цифровому світі. Характеристики набору тексту, дозвіл екрана нашого комп'ютера, смартфона або планшета, улюблені програми або веб-сайти та багато іншого є нашими цифровими слідами, які характеризують нас не менше, ніж наші звички для шахраїв в онлайн-середовищі. Рішення по аналітиці поведінки користувачів (UBA) здатні розпізнавати і диференціювати користувачів в залежності від їх цифрової активності.

Збираючи дані про поведінку користувачів і аналізуючи їх, інструменти UBA будують модель типового поведінки користувачів і дозволяють виявляти аномальне з точки зору безпеки поведінку. Постійне порівняння фактичної активності з цифровими відбитками кожного користувача дозволяє рішеннями виявляти підозрілу активність, пов'язану з атакою.

1.4. Аналіз технологій захисту привілейованого доступу користувачів інформаційної системи організації

Для вибору технології привілейованого доступу скористуємось звітом Gartner, які визначають управління привілейованим доступом як «основну технологію безпеки для захисту облікових записів, облікових даних і операцій, та пропонують підвищений («привілейований») рівень доступу [5]. Привілейований доступ, на відміну від звичайного доступу може вирішувати функції безпеки або

обслуговування, змінювати конфігурацію системи або додатки або обходити встановлені заходи безпеки через доступ суперкористувача.

Gartner охоплює три окремі категорії інструментів, які стали основним напрямком діяльності лідерів в області безпеки та управління ризиками (SRM- security and risk management), що розглядають можливість інвестування в інструменти PAM:

Привілейований аккаунт і управління сесіями (PASM - Privileged account and session managemen). Привілейовані облікові записи захищені сховищем їх облікових даних. Потім доступ до цих облікових записів здійснюється користувачами, службами та додатками-людьми. Функції привілейованого управління сеансом (PSM - Privileged session management) встановлюють сеанси з можливим введенням облікових даних і повним записом сеансу. Паролі та інші облікові дані для привілейованих облікових записів активно управляються, наприклад змінюються через певні інтервали часу або при виникненні певних подій. Рішення PASM також можуть управляти (міняти) облікові дані для облікових записів служб.

Управління підвищенням привілеїв і делегуванням (PEDM - Privilege elevation and delegation management). У керованій системі агенти хоста надають певні привілеї увійшов в систему користувачам. Інструменти PEDM забезпечують управління командами (фільтрацію) на основі хоста і підвищення привілеїв для серверів, останнім в формі дозволу виконання певних команд з більш високим рівнем привілеїв. Інструменти PEDM повинні виконуватися в реальній операційній системі (на рівні ядра або процесу). В інструменти UNIX / Linux PEDM часто включається функція мосту каталогів, що дозволяє користувачам входити в системи UNIX / Linux зі своїми обліковими даними Active Directory (AD). Управління командами через моніторинг сеансу (Фільтрація команд в сеансах Secure Shell [SSH]) явно виключено з цього визначення, оскільки точка управління менш надійна.

Секрети управління (SM - Secrets management.) Секрети (такі як паролі, токени OAuth, ключі SSH та інші облікові дані) для програмного забезпечення і машин програмно управляються, зберігаються і витягуються через API і комплекти розробки

програмного забезпечення (SDK). Довіра встановлюється і підтримується з метою обміну секретами і управління авторизацією і пов'язаними функціями між різними нелюдськими об'єктами, такими як машини, контейнери, додатки, служби, сценарії, процеси та конвеєри DevSecOps. Управління секретами часто використовується в динамічних і гнучких середовищах, таких як IaaS, PaaS і платформи управління контейнерами. Продукти для управління секретами також можуть забезпечувати управління паролями між додатками (AAPM).

Рис.1.7. Магічний квадрант управління привілейованим доступом

ARCON

ARCON - лідер в цьому магічному квадраті. Його продукт ARCON Privileged Access Management поставляється у вигляді пристрою, програмного забезпечення або

SaaS і забезпечує можливості сховища і PASM, функціональність PEDM для Windows і UNIX / Linux, а також управління секретами.

ARCON зосереджений на скороченні розриву з іншими постачальниками з повним пропозицією на основі SaaS і поліпшенням своїх функцій для підтримки Інтернету речей (IoT) і операційних технологій (OT).

Сильні сторони

Інновації: розробка продуктів ARCON значно просунулася з моменту оцінки для видання Magic Quadrant за 2020 рік, чому сприяли великі інвестиції. У ARCON є агресивна дорожня карта, яка включає додаткову підтримку OT і IoT, а також управління для ботів, додаткову інтеграцію роботизованої автоматизації процесів (RPA) і підтримку управління привілейованим доступом для інструментів DevOps.

Підтримка: ARCON не робить різниці між різними рівнями технічної підтримки. Вони пропонують цілодобову підтримку для всіх клієнтів в якості основного надання допомоги.

Ціни на програмне забезпечення: ціни на програмне забезпечення ARCON нижчі за середні по галузі для більшості оцінених сценаріїв ціноутворення. Однак ARCON стягує плату як за кількість користувачів, так і за кількість цільових систем, що може означати зростання витрат при значній зміні однієї з метрик.

BeyondTrust

BeyondTrust - лідер в цьому магічному квадраті. Він пропонує можливості PASM в рамках своєї пропозиції Password Safe в вигляді програмного забезпечення, фізичного або віртуального пристрою або SaaS. Він також пропонує продукт управління секретами DevOps Secrets Safe як програмного забезпечення. Можливості PEDM надаються через Управління привілеями для Windows, Управління привілеями для Mac і Управління привілеями для UNIX і Linux.

У BeyondTrust також є кілька додаткових продуктів, які частково збігаються з пропозицією PAM, які не оцінюються в цьому Magic Quadrant: активно продається продукт PASM під назвою Privileged Remote Access і два застарілих продукти, які

підтримуються, але не продаються активно (продукт PASM під назвою Privileged Identity і продукт PEDM під назвою PowerBroker для Windows).

BeyondTrust працює над додаванням функцій управління правами хмарної інфраструктури (CIEM).

Сильні сторони

Виявлення облікових записів: відмінні функції виявлення облікових записів доступні через надбудову BeyondInsight, яка входить до складу продуктів BeyondTrust PAM.

Панелі моніторингу / звіти: продукти BeyondTrust PAM виділяються своєю функцією звітності, яка включає в себе широкий список попередньо налаштованих шаблонів звітів і панелей візуалізації. Платформа також дозволяє адміністраторам створювати власні настроюювані інформаційні панелі з визначених шаблонів.

Управління додатками Windows: елементи управління додатками в інструменті BeyondTrust Privilege Management для Windows дуже надійні, з великим списком критеріїв для визначення та управління доступом до додатків. Крім того, інструмент Privilege Management для Mac надає повний набір елементів управління додатками для macOS.

Centrify

Centrify - лідер в цьому магічному квадраті. Служба привілейованого доступу Centrify доступна як SaaS і орієнтована на PASM, тоді як служба підвищення привілеїв Centrify має можливості PEDM. Постачальник також пропонує мости каталогів через Centrify Authentication Service.

Centrify традиційно орієнтувалася на AD, але тепер її технологія може використовуватися з іншими серверами каталогів.

На початку 2021 року, після дати закінчення цього дослідження, Centrify була придбана TPG, приватною інвестиційною компанією, і оголосила про злиття з Thycotic. Оцінка компанії Gartner компанії Centrify в цьому магічному квадраті відображає її позицію до придбання і злиття.

Сильні сторони

Мостове з'єднання каталогів: Centrify пропонує кращу в своєму класі можливість мостового з'єднання каталогів для UNIX і Linux і підтримує складні конфігурації AD.

Клієнтський досвід: клієнти Centrify високо оцінюють підтримку, а постачальник пропонує великі програми підтримки і навчання. Всі керівництва доступні онлайн без реєстрації.

Інтеграція: Centrify пропонує зрілі API-інтерфейси і має безліч готових інтеграцій з іншими інструментами безпеки, а також з інструментами DevOps, RPA і управління IT-послугами (ITSM).

Машинна аутентифікація: функція, названа як делеговані машинні облікові дані, спрощує процес аутентифікації для ідентифікації машин. Вона також забезпечує безпечний, обмежений підхід для міжмашинної аутентифікації без необхідності прямого доступу додатків до облікових даних у відкритому вигляді.

Softline рекомендує рішення One Identity Safeguard - це інтегроване рішення, що поєднує в собі можливості безпечного сховища паролів, централізованого управління сесіями, а також виявлення та аналізу загроз. Воно надійно записує, аналізує, зберігає і управляє обліковими даними привілейованих користувачів.

Основні сценарії використання One Identity Safeguard:

персоніфікація доступу до інформаційних систем;

контроль доступу до критичної інфраструктури;

виявлення скомпрометованих акаунтів;

запис сесій і створення доказової бази;

організація доступу віддалених бізнес-користувачів;

примус до проведення робіт в вікна обслуговування;

контроль доступу зовнішніх підрядників.

Тож надалі продовжимо дослідження технології One Identity Safeguard.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ДАНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Склад та основне призначення функціональних модулів One Identity Safeguard

One Identity Safeguard для Privileged Passwords 3000 і 2000 пристроїв створено спеціально для використання програмного забезпечення привілейованого управління Safeguard for Privileged Passwords, яке попередньо встановлено і готове до негайного використання. Пристрій призначено, щоб гарантувати безпеку системи на рівні обладнання, операційної системи і програмного забезпечення. Підхід з посиленим пристроєм захищає програмне забезпечення для привілейованого управління від атак, спрощуючи розгортання і поточне управління, а також скорочуючи терміни окупності.

Пакет програмного забезпечення для привілейованого управління Safeguard

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

До основних переваг продуктів Safeguard відноситься:

Універсальне рішення для забезпечення управління привілейованим доступом;

Легко розгортається і інтегрується;

Функції запису сесій;

Комплексний аналіз ризиків;

Управління привілейованої обліковим записом.

У комплект входять наступні модулі:

Safeguard for Privileged Password автоматизує, контролює та захищає процес, що забезпечує доступність привілейованих облікових даних за допомогою управління доступом на основі ролей та автоматизованих робочих процесів. Safeguard for Privileged Passwords, який захищає пристрої, усуває небезпеку за допомогою безпечного доступу до єдиного рішення. Це допомагає прискорити інтеграцію з інформаційною системою організації та IT-стратегіями. Крім того, його інтерфейс користувача дає можливість керувати паролями з будь -якого місця та за допомогою практично будь-якого пристрою. Результатом є рішення, яке захищає організацію та надає привілейованим користувачам новий рівень свободи та функціональності.

One Identity for Privileged Sessions є частиною портфеля управління привілейованим доступом One Identity. Удосконалення потреб великого підприємства, Safeguard for Privileged Sessions представляє собою рішення щодо управління привілегованими сеансами, які забезпечують кращі показники в галузі контролю доступу, а також моніторингу та записів сеансів для запобігання неправомірному використанню привілейованих облікових записів, забезпечення відповідності та прискорення випробувань.

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

One Identity Safeguard for Privileged Analytics об'єднує дані із Safeguard для Privileged Sessions, щоб використовувати їх у якості основи для аналізу подій, привілейованих користувачів. Захист для привілейованої аналітики використовує алгоритми машинного навчання для вивчення конкретних характеристик та створює профілі для кожного окремого привілейованого користувача. Захист для привілейованої аналітики порівнює фактичну активність користувачів із профілями користувачів у режимі реального часу, а профілі постійно коректуються за допомогою машинного навчання. Захист для привілейованої аналітики виявляє аномалії та

ранжує їх за ступенями ризику, це дозволяє розкладати пріоритети та розпочати відповідні дії та, у зв’язку з цим, запобігти витоку даних.

Як було відзначено раніше, дана привілейований доступ сфокусовано на трьох модулях [6]:

Safeguard for Privileged Passwords (SPP) - управління паролями;

Safeguard for Privileged Sessions (SPS) - управління сесіями;

Safeguard for Privileged Analytics (SPA) - аналіз поведінки.

Архітектура взаємозв'язку модулів представлено на рис.2.1.

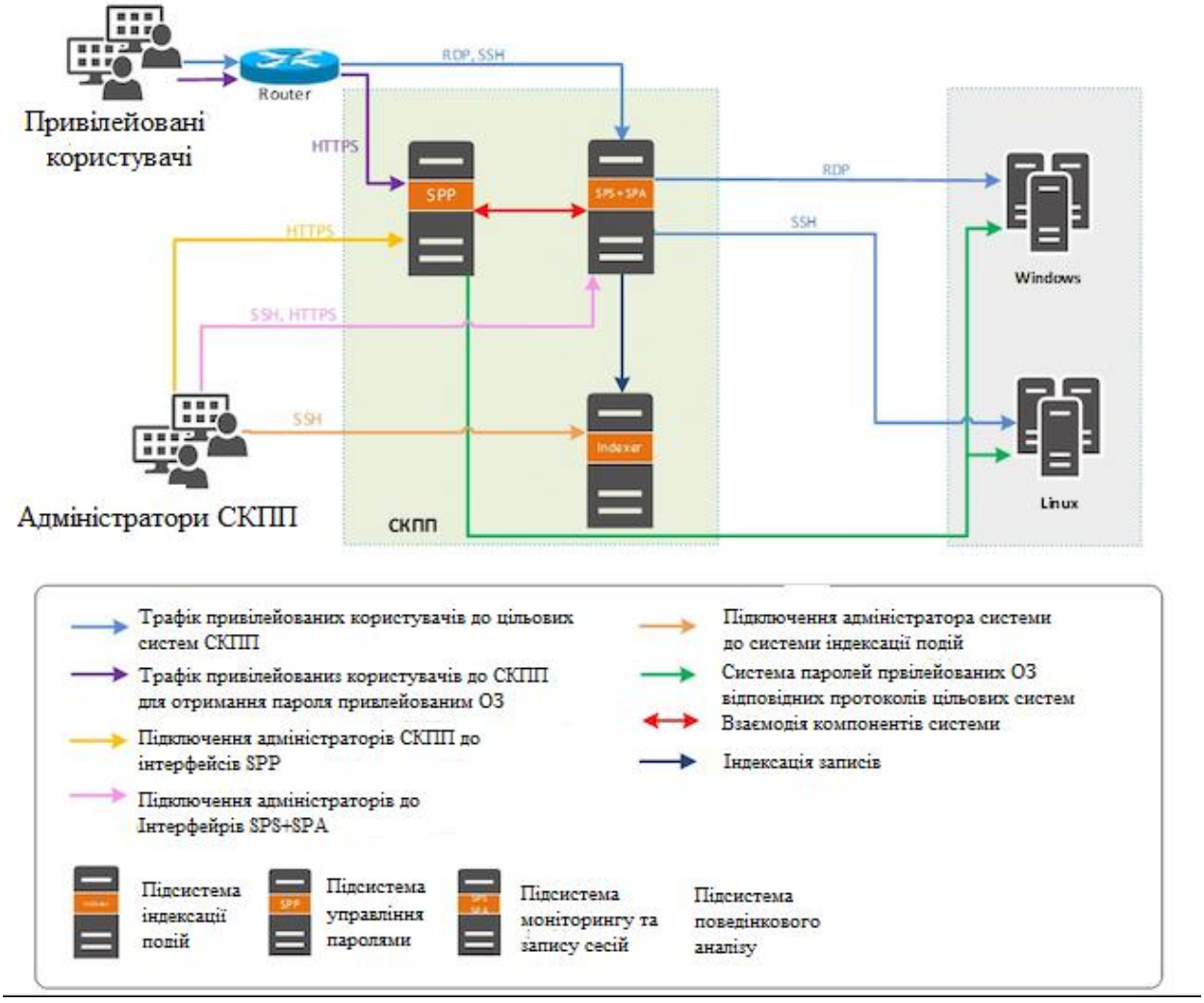


Рис.2.1. Архітектура захисту привілейованих користувачів

Для спрощення кожен з модулів представлений у вигляді одного блоку. Природно, продукт дозволяє створювати відмовостійкі конфігурації. Важливо відзначити, що One Identity Safeguard працює на мережевому рівні без необхідності установки агентів на кінцеві машини. Дана особливість дозволяє підвищити комфортність використання продукту, так як адміністраторам та підрядникам не потрібно буде переводити їх на використання незручних для них інструментів, а також прискорить час впровадження як для проведення тестових випробувань, так і в режимі робочої експлуатації для постійного функціонування.

Архітектура рішення Safeguard привілейованого доступу показано на рисунку 2.2.

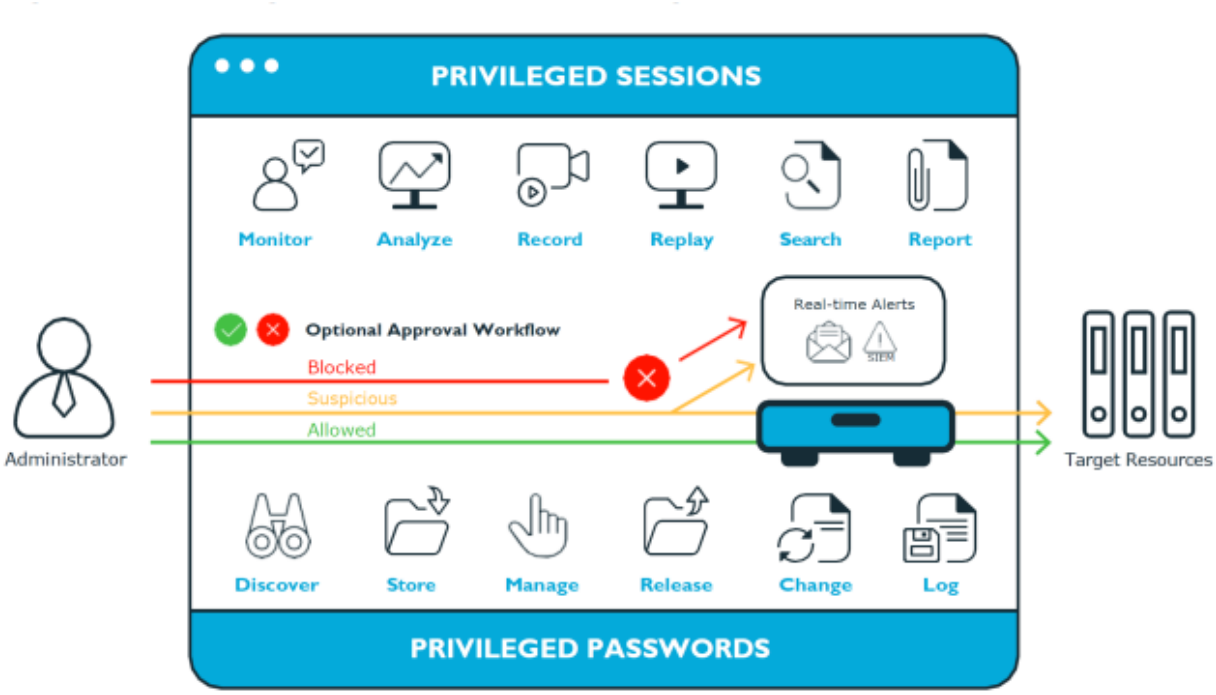


Рис.2.2. Архітектура привілейованого доступу Safeguard

Тож надалі визначимо призначення кожного з модуля.

2.2. Склад та функції логічних об’єктів Safeguard for Privileged Passwords

До складу логічних об’єктів Privileged Passwords входять (рис2.3) сховище паролів, ключів і секретів для захисту активів, включаючи комп'ютери, сервери, мережеві пристрої, каталоги та програми.

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

До логічних об’єктів належать комп’ютери, сервери, мережеві пристрої, каталоги або програми, якими може керувати Safeguard. Об’єкти мають пов’язані облікові записи користувачів та облікові записи служб. Активи та рахунки можуть бути імпортовані (наприклад, з Active Directory). Активи можуть бути або не бути частиною групи активів.

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

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

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

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

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

У наведеному нижче прикладі розділ А має три профілі (профіль А, В та С) та стандартний профіль. Профіль А перевіряє паролі кожні 30 днів. Профіль В перевіряє паролі кожні три місяців, а профіль С має найвищий рівень безпеки, перевіряючи паролі кожні сім днів. Як видно з рис.2.2 Сервер ресурсів має два профілі, кожен з яких керує різними обліковими записами пов'язані з активом. Профілі А, В і С явно призначаються обліковим записам та показаним активам. Хмарний сервіс не має активів чітко призначених профілю, тому файл за замовчуванням буде використовуватися для управління обліковими записами активу.

Визначимо що представляють собою активи і групи активів.

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

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

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

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

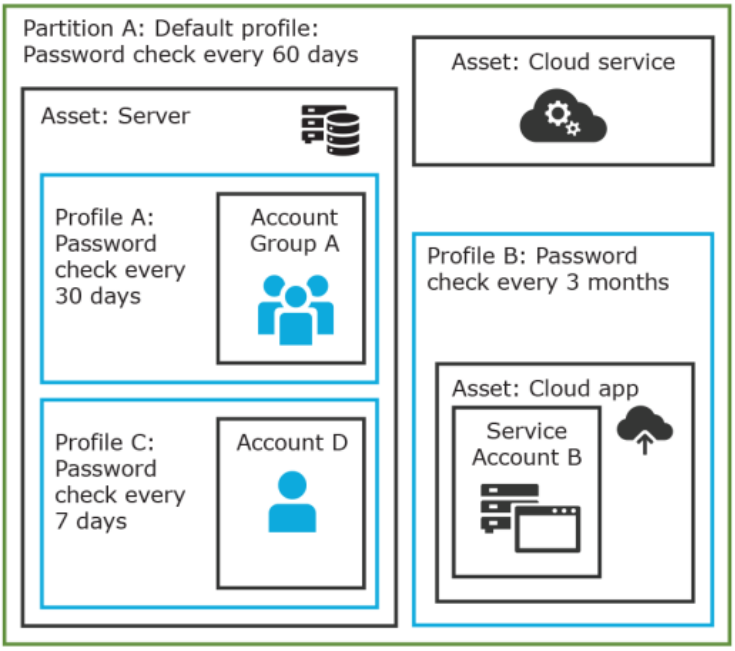


Рис. 2.2. Контроль паролів: розділ, профіль актив

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

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

Визначимо що представляють собою розділи та профілі.

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

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

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

2.3. Склад та функції логічних об’єктів Privileged Sessions

One Identity Safeguard for Privileged Sessions (SPS) є частиною рішення One Identity Safeguard, яке, у свою чергу, є частиною рішення управління привілейованим доступом One Identity. Для задоволення потреб великих підприємств SPS-це привілейоване рішення для управління сеансами, яке забезпечує кращий в галузі контроль доступу, запис сеансів та аудит для запобігання зловживанню привілейованими обліковими записами та прискорення розслідувань.

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

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

Визначимо основні характеристики SPS:

Централізоване застосування політик.

SPS діє як централізована точка автентифікації та контролю доступу в IT-середовищі, яке захищає від привілейованих крадіжок особистих даних та

зловмисників. Детальне управління доступом допомагає контролювати, хто і коли може отримати доступ до ваших критичних IT -ресурсів.

Запобігання зловмисним діям

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

Велика відповідальність (стримування)

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

Швидкі та економічні перевірки відповідності

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

Зниження витрат на пошук і усунення несправностей і проведення розслідувань

Коли щось відбувається не так, всі хочуть знати справжню історію. Аналіз тисяч текстових журналів може бути нескінченим і може викликати участь зовнішніх експертів. Можливість легко відновити сеанси користувачів дозволяє скоротити час дослідження і уникнути непередбачених витрат.

Особливості застосування та роботи SPS

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

Для реалізації рішення достатньо 3-5 днів!

Впровадження та налаштування відбувається без залучення дорогих професійних послуг.

Після розгортання SPS працює у фоновому режимі, як чорний ящик літака - для його роботи немає необхідності в додатковому робочому навантаженні.

SPS -незалежний пристрій без агентів.

У порівнянні з рішеннями на основі агентів немає необхідності в установці і оновленні агентів на клієнтах або серверах, що виключає непотрібне обслуговування і потенційні проблеми з безпекою. В якості шлюзу, незалежного від хоста, SPS може контролювати і відслідковувати доступ до будь-яких типів систем, в т.ч. всі сервери Windows / UNIX / Linux, мейнфрейми, мережеві пристрої, пристрої безпеки, веб-додатки або середовища тонких клієнтів, такі як VMware Horizon View (раніше відома як VMware View), Citrix Virtual Apps (раніше відома як Citrix XenApp) або Citrix Віртуальні робочі столи (раніше відомі як Citrix XenDesktop).

SPS прозорий, «роутерний» режим роботи.

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

Детальний контроль доступу

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

Запобігання шкідливих дій в режимі реального часу

SPS може відстежувати переданий контент в режимі реального часу і може відправляти попередження або навіть блокувати з'єднання, якщо в трафіку виявляється певний шаблон. Зумовлені шаблони можуть бути небезпечною командою в текстовому протоколі або підозрілим додатком в графічному з'єднанні. Ця політика на рівні команд і додатків може запобігати зловмисні дії користувачів у міру їх виникнення, а не просто записувати їх або повідомляти про них.

Запис і аудит сесій

SPS - це рішення для аудиту сеансів, що пропонує можливості оптичного розпізнавання символів (OCR) для реєстрації всіх даних про привілейовані дії в графічних додатках для інтерфейсів користувача, а також в текстових протоколів. SPS також може підтримувати і перевіряти передачу файлів. Всі дані записуються в журнали аудиту, схожі на фільми, з можливістю пошуку, що спрощує пошук необхідної інформації в розслідуваннях інциидентів або в ситуаціях, пов'язаних з усуненням неполадок. У разі будь-яких проблем (неправильна конфігурація сервера, маніпуляції з базою даних, несподіване завершення роботи) обставини події легко

доступні в журналах аудиту, тому причину інциденту можна легко визначити. Аудитори можуть виконувати пошук по довільному тексту в змісті текстових і графічних сеансів. Вони можуть шукати кожну подія (наприклад, клацання миші, натискання Enter) і тексти, які бачить користувач.

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

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

Можливі такі режими роботи:

Непрозорий проксі, який найпростіше реалізувати.

У цій конфігурації клієнти підключаються до сервера через SPS. Тобто кінцеві користувачі явно звертаються до SPS, який потім перенаправляє підключення до цільових систем на основі різних параметрів.

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

Прозорий режим з одним інтерфейсом.

Непрозора робота проксі

У цьому керівництві основна увага приділяється роботі непрозорого проксі, яку найпростіше реалізувати.

У цій конфігурації клієнти підключаються до сервера через SPS. Тобто кінцеві користувачі явно звертаються до SPS, який потім перенаправляє підключення до

цільових систем на основі різних параметрів залежно від того, який метод вибору місця призначення ви вибрали.

2.4. Склад та функції логічних об’єктів Privileged Privileged Analytics

SPS і SPA є частиною рішення One Identity Safeguard, яке, в свою чергу, є частиною рішення управління привілейованим доступом One Identity.

One Identity Safeguard для привілейованих сеансів (SPS) об'єднує дані з SPS, щоб використовувати їх в якості основи для аналізу поведінки користувачів. SPA використовує алгоритми машинного навчання для вивчення поведінкових характеристик (з використанням даних з SPS) і генерує профілі поведінки для кожного окремого привілейованого користувача. SPA порівнює фактичну активність користувачів з профілями користувачів в режимі реального часу, причому профілі постійно коригуються за допомогою машинного навчання. Коли SPA виявляє незвичну активність, це відображається в інтерфейсі SPS у вигляді високих балів і візуалізованою інформацією [7].

Тож зауважимо, що SPA працю в поєднанні з SPS. Визначимо вимоги для нормальної роботи SPA:

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

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

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

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

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

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

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

Алгоритми One Identity Safeguard для Privileged Analytics є математичні методи, які можна використовувати для аналізу даних сеансу з різних сторін. Алгоритми необхідно навчати з використанням історії даних сеансу. На основі цього навчання алгоритм може побудувати базову лінію поведінки конкретного користувача і оцінити нові сеанси. Бали такої оцінки покажуть, чи є поведінка конкретного користувача нормальною або аномальною в порівнянні з базовим рівнем. Алгоритми також забезпечують візуалізацію для відображення інформації про поведінку користувача [10].

В даний час підтримуються наступні алгоритми Privileged Analytics:

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

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

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

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

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

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

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

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

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

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

Що стосується розміру часових проміжків і того, наскільки великий проміжок кваліфікується як проміжок часу, що заслуговує моніторингу, алгоритм вважає час, що минув між двома сеансами, якщо довжина проміжку дорівнює або більше 10 хвилин або менше двох днів.

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

Оцінка алгоритму

Інструмент оцінки алгоритмів - це допоміжний інструмент, який використовується для оцінки того, наскільки добре алгоритми машинного навчання працюють для аналітики SPS з поточним набором даних, що знаходяться в рішенні SPS. Інструмент щодня автоматично запускається сервісом analytics-daily.service, але його також можна запустити вручну, виконавши такі команди на консолі за вказівкою One Identity Support:

make-cross-scores: ця команда виконує підрахунок балів, який служить основою для процедури оцінки алгоритму.

Assessment-cross-scores: ця команда оцінює показники оцінки, виконаної за допомогою команди make-cross-scores, і генерує звіт про оцінку, доступний за наступною адресою:

/ Opt / pam-pipeline / var / algoeval-report /

Каталог звітів містить результати оцінки в файлі report.txt і в декількох файлах графічних зображень у форматі * .png.

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

3 РОЗРОБЛЕННЯ ВАРІАНТУ ТЕХНОЛОГІЇ РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ РІШЕННЯ ONE IDENTITY SAFEGUARD ПРИВІЛЕЙОВАНОГО ЗАХИСТУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1. Технологія налаштування Safeguard for Privileged Passwords

Розглянемо робочий процес запиту доступу Safeguard for Privileged Passwords

На високому рівні кінцевий користувач або користувальницький додаток інтеграції може відправити запит на доступ до:

Облікових даних(пароль або SSH-ключ), якими керує Safeguard for Privileged Passwords.

Сеанс (наприклад, RDP, SSH або Telnet) з активом, яким управляє Safeguard for Privileged Passwords з додаванням Safeguard for Privileged Sessions

Запит на доступ може бути наданий негайно або може спочатку пройти процес затвердження.

Після підтвердження облікових даних або сеансу можна перевірити і використовувати отримані доступи. Для сеансів всі підключення проксіруются через Safeguard для привілейованих сеансів і записуються.

Після використання облікових даних або сеансу їх можна перевірити, щоб підтвердити, що користувач закінчив роботу. Політику запиту доступу потім можна налаштувати так, що потрібна перевірка запиту перед повторною перевіркою. Для запитів типу облікових даних політика запиту доступу також може бути налаштована для зміни облікових даних [7].

Для привілейованих паролів доступні наступні функції представлені в таблиці 3.1.

Таблиця 3.1.

Можливості One Identity Safeguard for Privileged Passwords

Характеристика	Опис
Автоматична авторизація	Автоматичний вхід в систему і запуск запиту доступу до сеансу підвищує безпеку і відповідність вимогам, оскільки облікові дані облікового запису ніколи не розкриваються користувачеві.
Activity Center	Використовуючи Activity Center, можна швидко і легко переглянути всі дії, які виконуються користувачами Safeguard for Privileged Passwords, і інтегровані процеси. У звітах Activity Center можна виконувати пошук, налаштовувати і фільтрувати дані, щоб зосередити увагу на діях одного користувача або для аудиту багатьох дій в підмножині відділів. Крім того, можна запланувати запити, а також зберегти або експортувати дані.
Завжди онлайн	Захист привілейованих паролів. Пристрої можуть бути об'єднані в кластер для забезпечення високої доступності. Паролі, ключі SSH і сеанси можна запросити з будь-якого пристрою в кластері Safeguard for Privileged Passwords. Така структура розподіленої кластеризації також забезпечує відновлення або продовження життєво важливої технологічної інфраструктури та систем після стихійних лих або антропогенних катастроф.

Підтвердження з будь-якого місця	Використовуючи One Identity Starling, можна схвалити або відхилити будь-який запит доступу в будь-якому місці, не перебуваючи в VPN.
Хмарна підтримка	Safeguard для привілейованих паролів можна запустити в хмарі за допомогою Azure або AWS.

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

Рисунок 3.1. Архітектура кластера SPP

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

Для створення привілейованих користувачів можливо використовувати інфраструктуру каталогів (наприклад, Microsoft Active Directory). Для цього необхідно

імпортувати користувачів каталогу та групи каталогу. Користувачі каталогу проходять автентифікацію в Safeguard for Privileged Passwords, використовуючи облікові дані каталогу. Користувачі керованих облікових записів не можуть бути членами групи безпеки AD «Захищені користувачі».

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

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

Список схем активів

Користувачі:

Ім'я користувача

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

Опис

Групи:

Ім'я

Член

Комп'ютер:

Ім'я

Мережева адреса

Операційна система

Версія операційної системи

Опис

Список схем постачальників ідентифікації та аутентифікації:

Користувачі

Ім'я користувача

Ім'я

Прізвище

Робочий телефон

Мобільний телефон

Ел. адреса

Опис

Перевірка автентичності зовнішньої федерації

Радіус аутентифікації

Керовані об'єкти

Групи:

Ім'я

Члени

Опис

Створення таких каталогів надасть можливисті покращеної роботи з привілейованими записами

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

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

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

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

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

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

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

Керування доступом на основі ролей (RBAC). Safeguard for Privileged Passwords використовує ієрархію керування доступом на основі ролей з використанням наборів дозволів адміністратора. Доступно безліч ролей для адміністрування Safeguard для привілейованих паролів, що забезпечують детальне делегування та робочі процеси, а також найменш привілейований доступ.

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

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

Підтримка двофакторної автентифікаціїю. Недостатньо захистити доступ до паролів іншим паролем. Підвищена безпека за рахунок вимоги двофакторної автентифікації для захисту привілейованих паролів. Safeguard for Privileged Passwords

підтримує будь-яке рішення 2FA на основі Radius та служби двофакторної аутентифікації (2FA) компанії One Identity.

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

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

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

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

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

Крок 1. Створіть адміністратора авторизатора

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

1. Адміністратор користувачів
2. Адміністратор служби підтримки

3. Адміністратор пристрою
4. Адміністратор операцій
5. Аудитор
6. Адміністратор активів
7. Адміністратор політики безпеки

Крок 3. Адміністратор пристрою налаштовує пристрій:

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

Налаштуйте параметри зовнішньої інтеграції, які застосовуються.

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

Ідентифікація та автентифікація: налаштуйте служби каталогів, такі як сервери Active Directory та LDAP, для використання як постачальників ідентифікації та автентифікації для користувачів Safeguard for Privileged Passwords . Налаштуйте Safeguard для привілейованих паролів як сторону, що перевіряє та використовує SAML 2.0 для інтеграції із зовнішніми службами для аутентифікації користувачів. Створіть сервер RADIUS, який буде використовуватися як первинний або вторинний провайдер аутентифікації.

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

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

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

Крок 4. Адміністратор користувачів додає користувачів

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

Крок 5. Адміністратор активів додає керовані системи

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

Правила використання пароля облікового запису

Зміна паролю

Перевірити пароль

Групи синхронізації паролів

4. Встановіть такі параметри керування ключами SSH за необхіднісю:

Змінити налаштування ключа SSH

Перевірте налаштування ключа SSH

Відкрийте для себе налаштування ключа SSH

Установки груп синхронізації ключів SSH

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

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

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

Крок 6. Адміністратор політики безпеки додає політики запитів на доступ

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

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

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

4. Додати групи користувачів (Додати групи користувачів).

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

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

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

8. Додати права (Додавання права).

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

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

3.2. Варіанти роботи One Identity Safeguard for Privileged Sessions

Варіанти або режими роботи One Identity Safeguard for Privileged Sessions (SPS) може бути налаштований для моніторингу як прозорих, так і непрозорих з'єднань.

У *прозорому режимі* SPS діє як прозорий маршрутизатор між двома сегментами мережі.

Можливо використовувати маршрутизацію на основі політик для перенаправлення з'єднань в одному сегменті мережі SPS, і в цьому випадку він діє як прозорий маршрутизатор з одним інтерфейсом.

У непрозорому режимі користувачі повинні звертатися до SPS, щоб почати підключення до захищених серверів.

При зверненні до SPS також можна використовувати вибір внутрішньосмугового призначення, щоб вибрати сервер для підключення.

One Identity рекомендує розробити топологію мережі так, щоб через SPS проходив лише трафік керування та адміністрування сервера. Це гарантує, що служби та програми, що працюють на серверах, доступні навіть у разі відмови SPS, тому SPS не може стати єдиною точкою відмови.

Розглянемо дані режими докладніше.

Прозорий режим

У прозорому режимі One Identity Safeguard для привілейованих сеансів (SPS) діє як прозорий маршрутизатор, що з'єднує мережевий сегмент адміністраторів із сегментом захищених серверів на мережному рівні (рівень 3 моделі OSI). Усі з'єднання повинні проходити через SPS, щоб досягти серверів - SPS - це проксі-шлюз, що повністю відокремлює захищені сервери від решти мережі. Контрольовані з'єднання та трафік перевіряються на рівні додатків, тоді як інші типи з'єднань просто перенаправляються на рівні пакетів (рис.3.2).

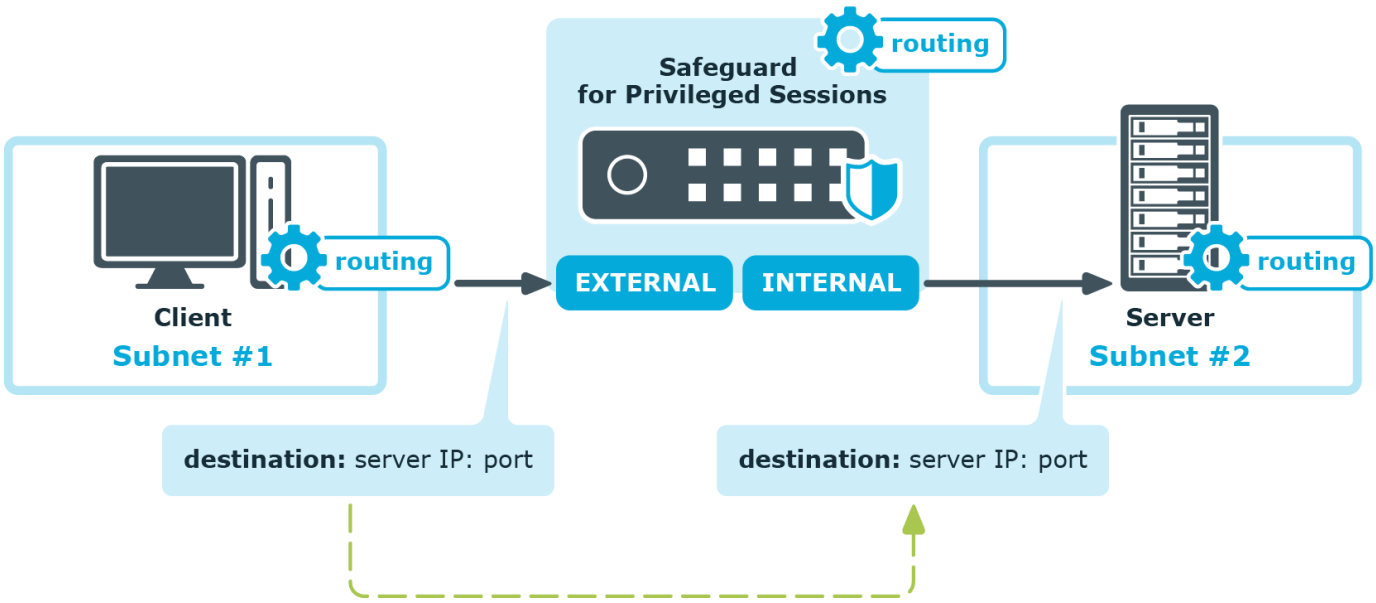


Рис. 3.2. Прозорий режим One Identity Safeguard for Privileged Sessions

Прозорий режим з одним інтерфейсом

Прозорий режим з одним інтерфейсом аналогічний прозорому режиму, але трафік на стороні клієнта та на стороні сервера використовує той самий інтерфейс. Потрібний зовнішній пристрій, який активно перенаправляє перевірений трафік у One Identity Safeguard for Privileged Sessions (SPS) (зазвичай це міжмережевий екран, маршрутизатор або комутатор рівня 3). Для цього зовнішній пристрій повинен підтримувати розширену маршрутизацію (також так звану маршрутизацію на основі політик або PBR).

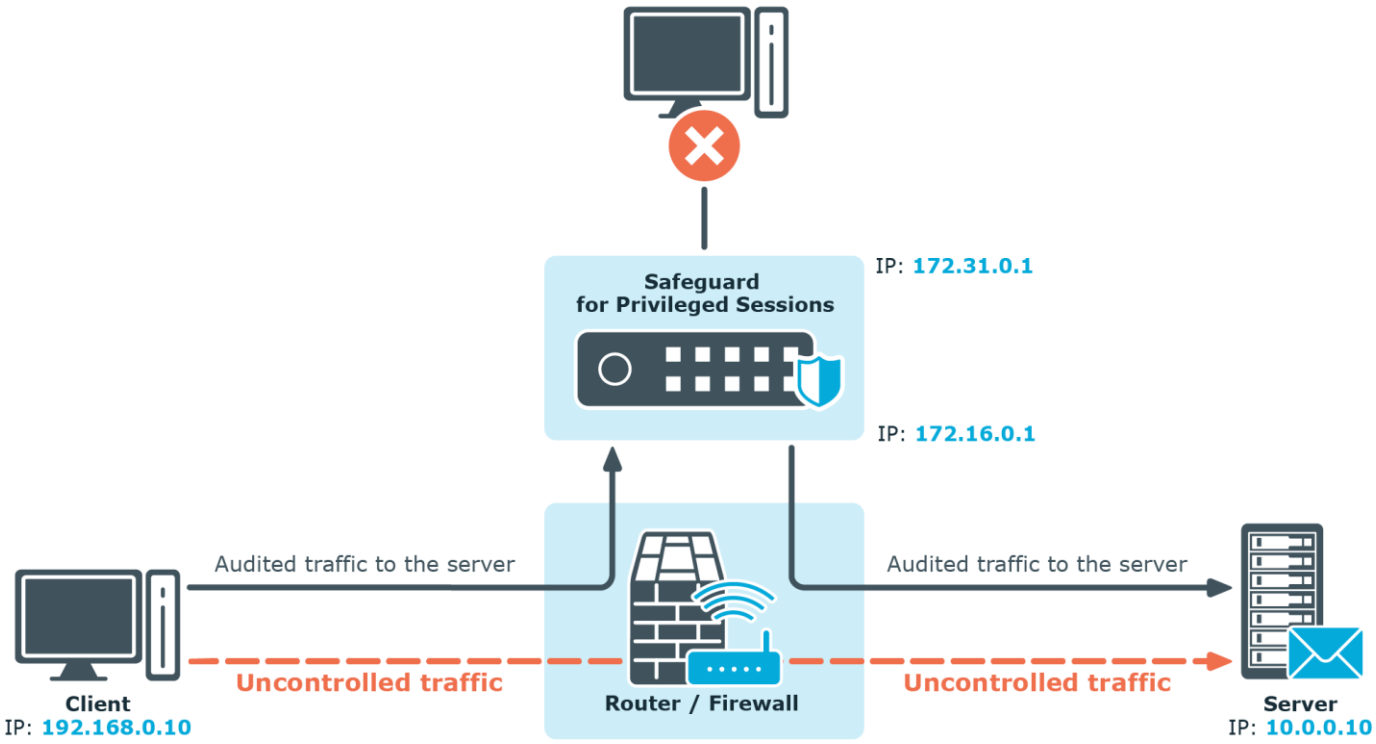


Рис.3.3. SPS у прозорому режимі з одним інтерфейсом

Переваги використання прозорого режиму з одним інтерфейсом:

Абсолютно прозорий для клієнтів, немає необхідності змінювати їхню конфігурацію.

Топологія мережі не змінилася.

На SPS направляється лише перевірений трафік, виробничий трафік – ні.

Недоліками використання прозорого режиму з одним інтерфейсом є:

SPS діє як посередник щодо з'єднання між клієнтом та цільовим сервером. Замість одного з'єднання клієнт-сервер існує два окремих з'єднання: перше між клієнтом та SPS, а друге між SPS та сервером. Залежно від того, як ви налаштовуєте SPS, вихідна IP-адреса у з'єднанні з SPS-сервером може бути IP-адресою SPS або IP-адресою клієнта. В останньому випадку – при роботі в прозорому режимі (у тому числі в прозорому режимі з одним інтерфейсом) – SPS виконує заміну IP.

У непрозорому режимі One Identity Safeguard для привілейованих сеансів (SPS) діє як хост-бастіон (тобто адміністратори можуть звертатися тільки до SPS, сервери,

що адмініструються, не можуть бути націлені безпосередньо). Брандмауер мережі має бути налаштований так, щоб лише з'єднання, що виходять від SPS, могли отримати доступ до серверів. SPS визначає, до якого сервера підключатися, ґрунтуючись на параметрах вхідного з'єднання (IP-адреса адміністратора, а також цільова IP-адреса та порт).

Непрозорий режим за своєю суттю гарантує, що лише контрольований (управління та адміністрування сервера) трафік досягає SPS. Служби та програми, що працюють на серверах, доступні навіть у разі виходу з ладу SPS, тому SPS не може стати єдиною точкою відмови.

Трафік повинен активно маршрутизуватись на SPS за допомогою зовнішнього пристрою. Отже, адміністратор мережі може вимкнути SPS, змінивши правила маршрутизації.

При додаванні нового порту або підмережі до списку підключень, що перевіряються, необхідно також змінити конфігурацію зовнішнього пристрою.

Мережевий адміністратор може (навмисно або ненавмисно) легко вимкнути моніторинг серверів, тому для виявлення таких дій необхідно вжити додаткових заходів.

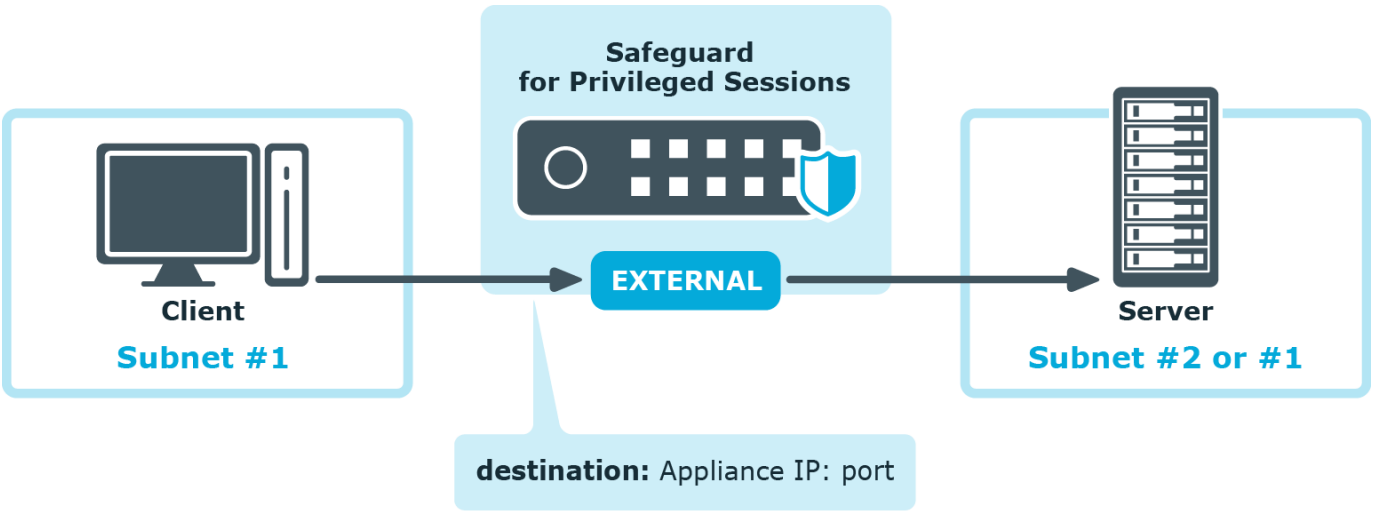


Рис.3.4. Непрозорий режим One Identity Safeguard for Privileged Sessions

Підключення до сервера через One Identity Safeguard для привілейованих сеансів (SPS).

Коли клієнт ініціює з'єднання з сервером, One Identity Safeguard для привілейованих сеансів (SPS) виконує процедуру, яка залежить від протоколу, який використовується при з'єднанні, а саме:

З’єднання з сервером через One Identity Safeguard для привілейованих сеансів (SPS) за допомогою SSH .

З'єднання з сервером через One Identity Safeguard для привілейованих сеансів (SPS) за допомогою RDP.

Доступ та налаштування One Identity Safeguard для привілейованих сеансів (SPS)

One Identity Safeguard для привілейованих сеансів (SPS) має веб-інтерфейс та налаштовується з браузера. Користувачі SPS можуть бути автентифіковані за допомогою локальних баз даних, баз даних LDAP або RADIUS (рис.3.5). Привілеї користувачів визначаються членством у групах, якими можна управляти або локально на SPS, або централізовано у базі даних LDAP. Призначення привілеїв групам ґрунтується на списках контролю доступу (ACL). Також можна зіставити групи, що існують у базі даних LDAP, з набором привілеїв SPS. Контроль доступу в SPS дуже докладний, можна точно визначити, хто може отримати доступ до яких частин інтерфейсу і збережених даних [9].

Safeguard for Privileged Sessions (SPS) може запускатися з хмари.

Перед тим, як почати вибирати платформи з яких запускати Safeguard for Privileged Sessions, визначте ресурси такі, як ЦП, доступність пам'яті, підсистема введення-виведення та мережна інфраструктура, щоб переконатися, що на віртуальному рівні [9].

Платформи з хмарним розгортанням:

Віртуальна машина AWS (BM)

Віртуальна машина Azure (BM).

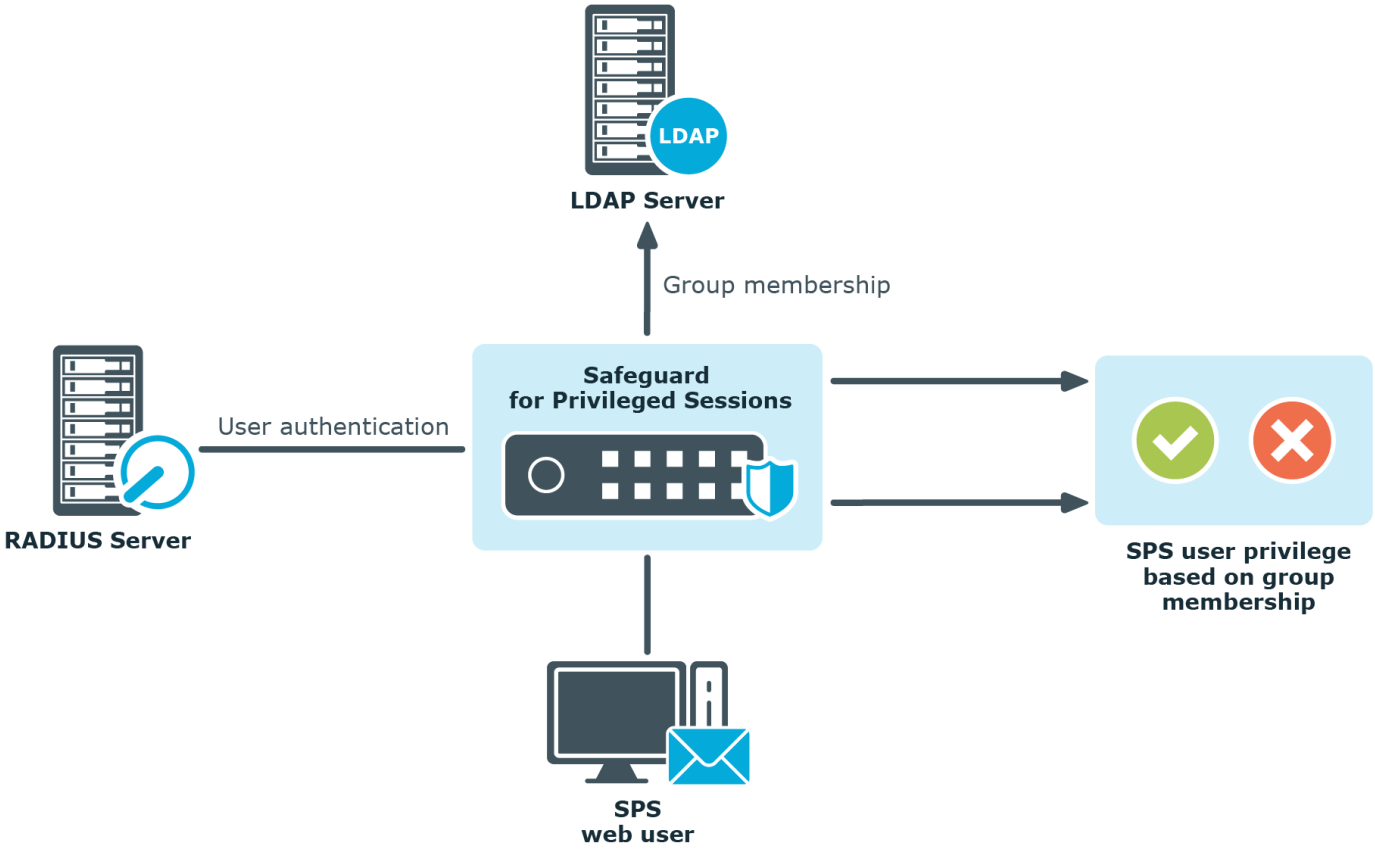


Рис. 3.5. Аутентифікація користувачів SPS

3.3. Технологія One Identity Safeguard for Privileged Analytics

Привілейована аналітика загроз дозволяє дізнатися, хто з ваших привілейованих користувачів є з високим ризиком, відстежувати сумнівну поведінку та виявляти раніше невідомі загрози всередині та за межами організації. Safeguard for Privileged Analytics виявляє аномалії та ранжує їх залежно від ступеня ризику, щоб була можливість розставити пріоритети та вжити відповідних дій - і зрештою запобігти витоку даних.

Для налаштування аналітики необхідно вибрати аналітику (також звані алгоритмами), яку ви хочете використовувати для аналізу даних сеансу, та увімкніти їх у SPS.

Дані сеансу оцінюються за допомогою будь-якої комбінації увімкнених алгоритмів. Оцінки, виставлені алгоритмами, підсумовуються для створення єдиної оцінки.

У процесі агрегування видаляються найнижчі та найвищі оцінки. Це необхідно для того, щоб знизити кількість помилкових спрацьовувань і помилково-негативних результатів. На типову атаку вказують ознаки незвичайної поведінки користувача, незвичайної з різних точок зору. Однак деякі речі зазвичай цілком нормальні навіть у найдивніших сеансах. Ось чому видалення оцінок на двох крайніх точках допомагає мінімізувати кількість хибних спрацьовувань та хибнонегативних результатів [10].

Щоб настроїти алгоритми SPS, виконайте такі дії.

1. У SPS перейдіть до Політики> Політики аналітики.

2. Введіть назву своєї аналітичної політики.

3. Для кожного алгоритму, виберіть одне з наступних значень:

Вимкнути : виберіть це значення, якщо ви не бажаєте використовувати певний алгоритм.

Використання : Виберіть це значення, якщо потрібно використовувати певний алгоритм.

Довіра : виберіть це значення, якщо ви хочете використовувати конкретний алгоритм і хочете включити до остаточної сукупної оцінки всі оцінки, отримані цим алгоритмом.

Пам'ятайте, що під час агрегування оцінок видаляються найнижчі та найвищі оцінки. Ви можете відмовитися від цього принципу, вибравши "Довіряти" для тих алгоритмів, яким ви хочете надати більшої ваги в підсумковій сукупній одиничній оцінці.

4. Параметр Виявлення сеансу за сценарієм увімкнено за замовчуванням. Вирішіть, чи хочете ви увімкнути виявлення сеансів за сценарієм. Виявлення сеансу за сценарієм виконується алгоритмом часового майстра.

5. Натисніть кнопку Здійснити.

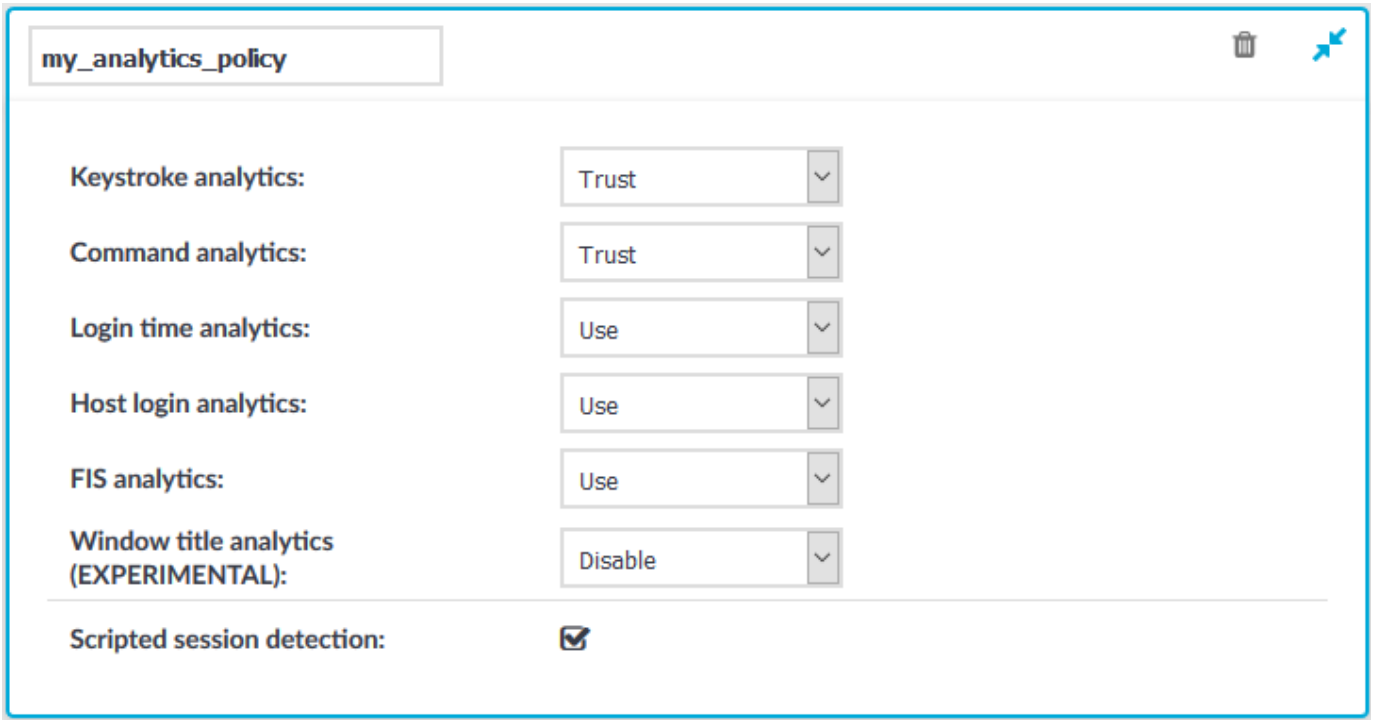


Рис. 3.6. Вибір політик аналітики

Для використання SPA, виконайте наведені нижче дії.

1. Побудуйте першу базову лінію. Ви можете зробити це одним із наступних способів:

Зачекайте, доки спрацює щоденна періодична будівля (запускається cron).

Увійдіть через SSH в ядро-оболонку, а потім введіть /opt/pam-pipeline/bin/build-baselines.

Для першого запуску рекомендується запустити його з -ld (журнал для консолі та налагодження), це не вплине на продуктивність.

Для завершення побудови базової лінії може знадобитися деякий час, якщо даних багато, тому є сенс запускати її на екрані з фіксованого вузла.

Побудова базового плану - це періодичний асинхронний процес, що означає, що вхідні сеанси не змінюють базовий план негайно.

2. Перевірте, чи побудовані базові лінії:

2.1 Підключіться до PostgreSQL, бази даних, де постійно зберігаються результати будь-якого аналізу, виконаного SPA, для подальшого відображення в інтерфейсі пошуку:

psql -U paa paa

2.2 Виконайте SQL-запити, щоб отримати список користувачів, для яких було створено базовий план:

Для алгоритму натискання клавіш використовуйте:

виберіть окремий user_id із натискання клавіші;

Для командного алгоритму використовуйте:

виберіть окремий user_id із команди;

Для алгоритму часу входу до системи використовуйте:

виберіть окремий user_id із часу входу до системи;

Для алгоритму входу до системи використовуйте:

виберіть окремий user_id з hostlogin;

Для алгоритму fis використовуйте:

виберіть окремий user_id із fis;

Для алгоритму заголовка вікна використовуйте:

виберіть окремий user_id із заголовка вікна;

Для алгоритму годинникового майстра використовуйте:

виберіть окремий user_id із clockmaster;

Підрахунок очок відбувається лише за наявності базового рівня.

3. Почніть набирати очки.

Оцінка відбувається в режимі реального часу, що означає, що як тільки доступні нові дані (навіть дані поточного сеансу), SPA негайно оцінює їх.

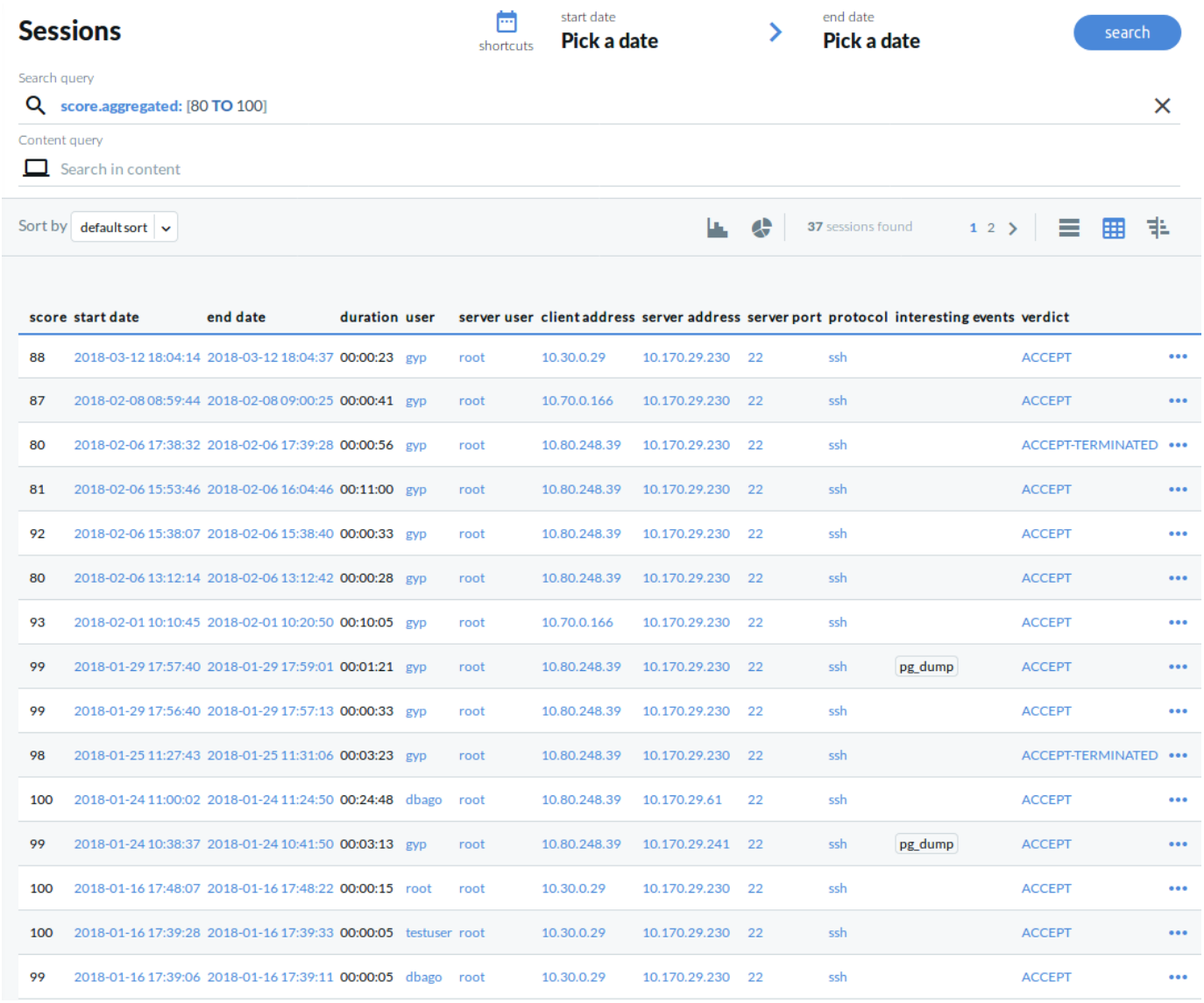
4. Пошук сеансів із високими балами.

4.1 Перейдіть до Search> Search .

Сеанси відображаються відсортованими за датою. Для поточних сеансів інтерфейс пошуку оновлюється в режимі реального часу, щоб завжди відображати останню інформацію.

4.2 У полі Пошуковий запит введіть score.aggregated: [від 80 до 100] і натисніть Пошук.

Оцінка від 80 до 100 вказує на незвичайну поведінку користувача.



score	start date	end date	duration	user	server user	client address	server address	server port	protocol	interesting events	verdict
88	2018-03-12 18:04:14	2018-03-12 18:04:37	00:00:23	gyp	root	10.30.0.29	10.170.29.230	22	ssh		ACCEPT
87	2018-02-08 08:59:44	2018-02-08 09:00:25	00:00:41	gyp	root	10.70.0.166	10.170.29.230	22	ssh		ACCEPT
80	2018-02-06 17:38:32	2018-02-06 17:39:28	00:00:56	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT-TERMINATED
81	2018-02-06 15:53:46	2018-02-06 16:04:46	00:11:00	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT
92	2018-02-06 15:38:07	2018-02-06 15:38:40	00:00:33	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT
80	2018-02-06 13:12:14	2018-02-06 13:12:42	00:00:28	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT
93	2018-02-01 10:10:45	2018-02-01 10:20:50	00:10:05	gyp	root	10.70.0.166	10.170.29.230	22	ssh		ACCEPT
99	2018-01-29 17:57:40	2018-01-29 17:59:01	00:01:21	gyp	root	10.80.248.39	10.170.29.230	22	ssh	pg_dump	ACCEPT
99	2018-01-29 17:56:40	2018-01-29 17:57:13	00:00:33	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT
98	2018-01-25 11:27:43	2018-01-25 11:31:06	00:03:23	gyp	root	10.80.248.39	10.170.29.230	22	ssh		ACCEPT-TERMINATED
100	2018-01-24 11:00:02	2018-01-24 11:24:50	00:24:48	dbago	root	10.80.248.39	10.170.29.61	22	ssh		ACCEPT
99	2018-01-24 10:38:37	2018-01-24 10:41:50	00:03:13	gyp	root	10.80.248.39	10.170.29.241	22	ssh	pg_dump	ACCEPT
100	2018-01-16 17:48:07	2018-01-16 17:48:22	00:00:15	root	root	10.30.0.29	10.170.29.230	22	ssh		ACCEPT
100	2018-01-16 17:39:28	2018-01-16 17:39:33	00:00:05	testuser	root	10.30.0.29	10.170.29.230	22	ssh		ACCEPT
99	2018-01-16 17:39:06	2018-01-16 17:39:11	00:00:05	dbago	root	10.30.0.29	10.170.29.230	22	ssh		ACCEPT

Рис.3.7. Сеанси з високими балами - перегляд таблиці

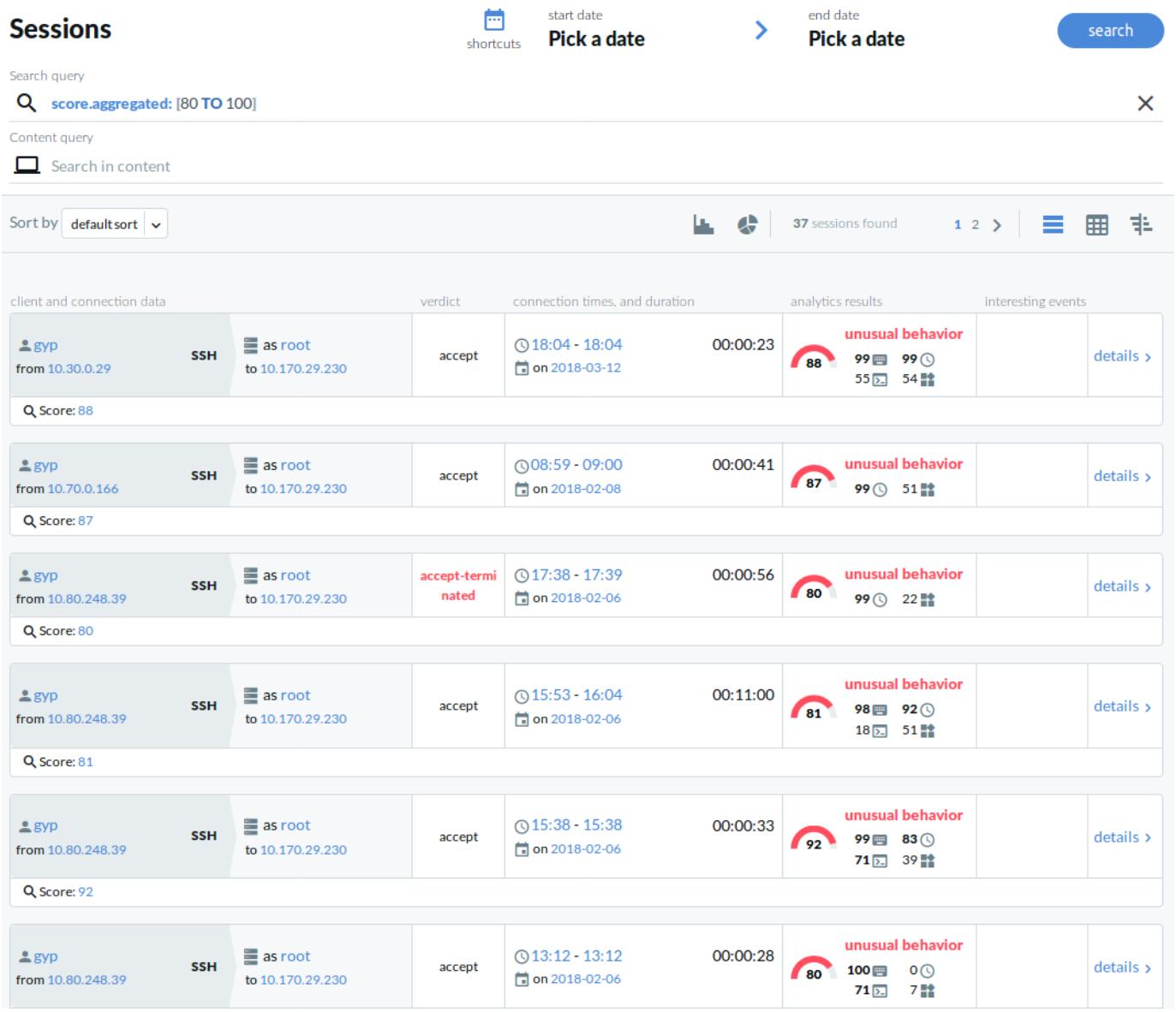


Рис.3.8. Сеанси з високими балами - перегляд карток

Зверху на сторінці відображається зведення основних відомостей про сеанс, наприклад:

Сумарний бал (вказується шкалою). Використовуються такі коди кольорів:

Бали від 80 до 100 вказують на незвичайну поведінку, їх колірний код – червоний.

Бали від 70 до 79 вказують на поведінку, яка може вимагати подальшого аналізу та уваги, їх колірний код – жовтий.

Бали від 0 до 69 вказують на нормальну поведінку, їх колірний код – сірий.

Короткий виклад вердикту кожного алгоритму про сеанс та поведінку користувача можна визначити в розділах «Виявлені аномалії» та «Нормальна поведінка», де відображається докладний аналіз, який надається кожним із налаштованих алгоритмів. Сюди входить коротка інформація, як працює конкретний алгоритм і як читати візуалізовану інформацію, і навіть бали, виставлені окремими алгоритмами [10, 11]..

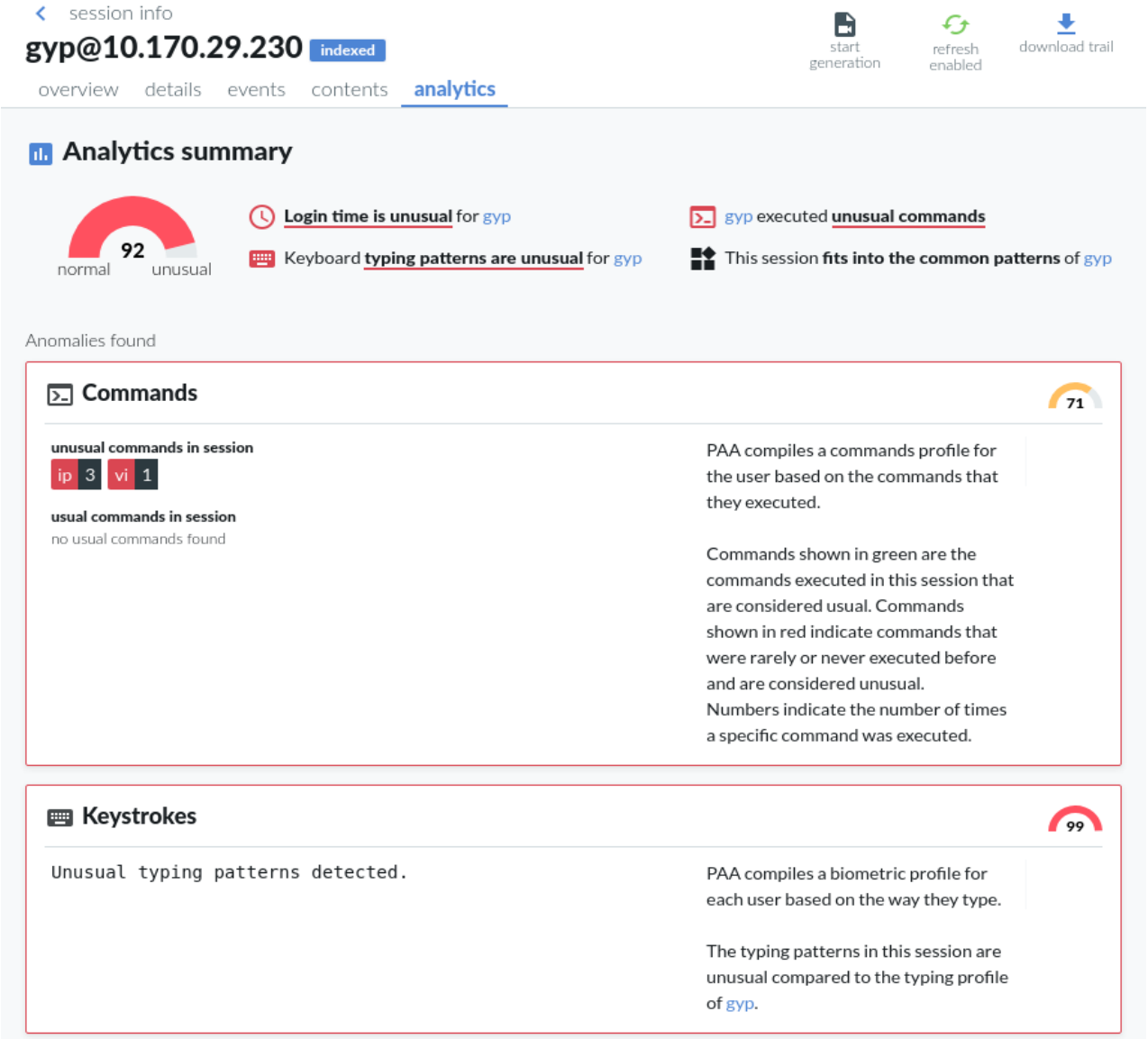


Рис. 3.9. Перегляд відомостей на вкладці аналітики: виявлені аномалії

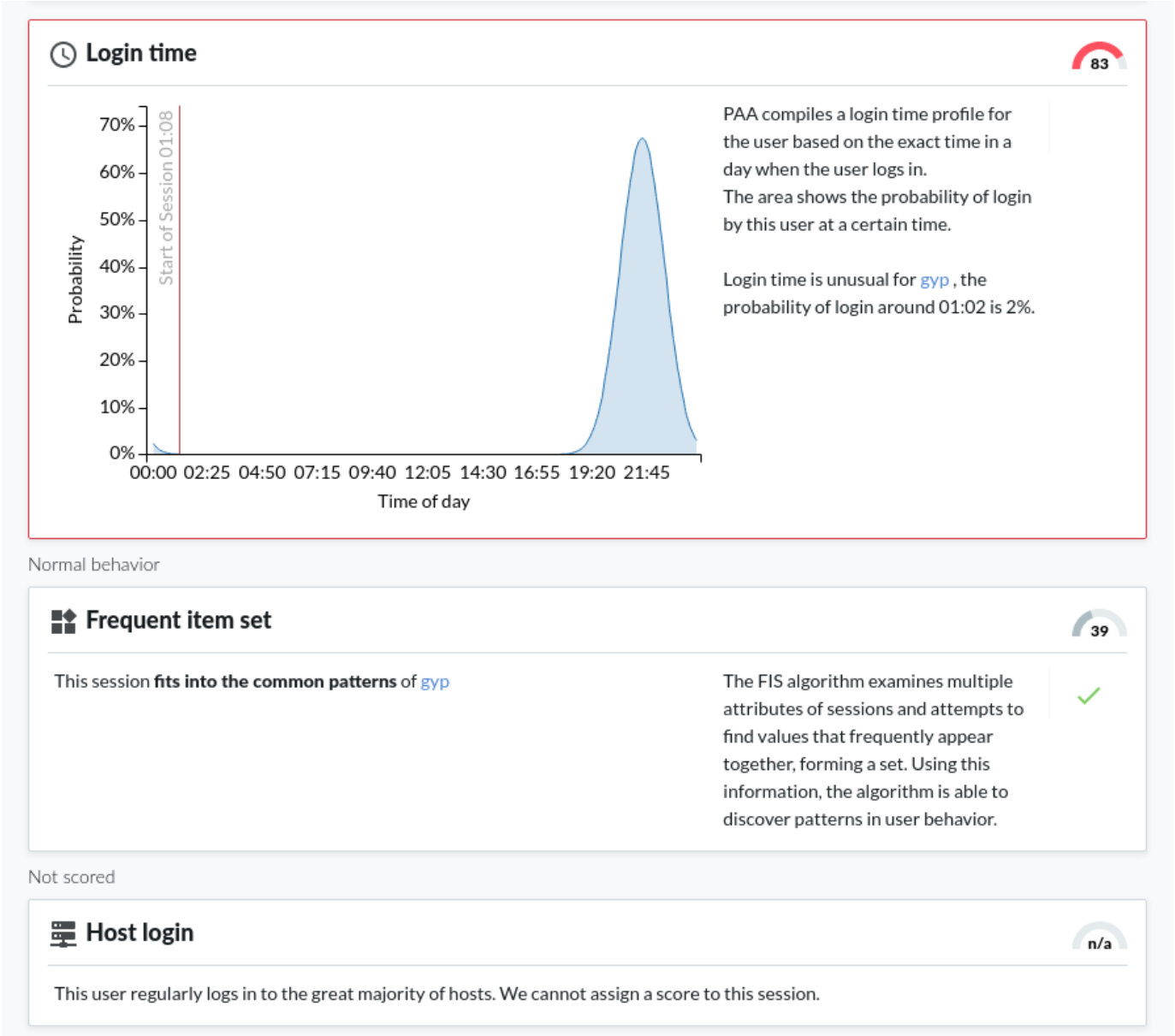


Рис.3.10. Перегляд відомостей на вкладці аналітики: виявлені аномалії

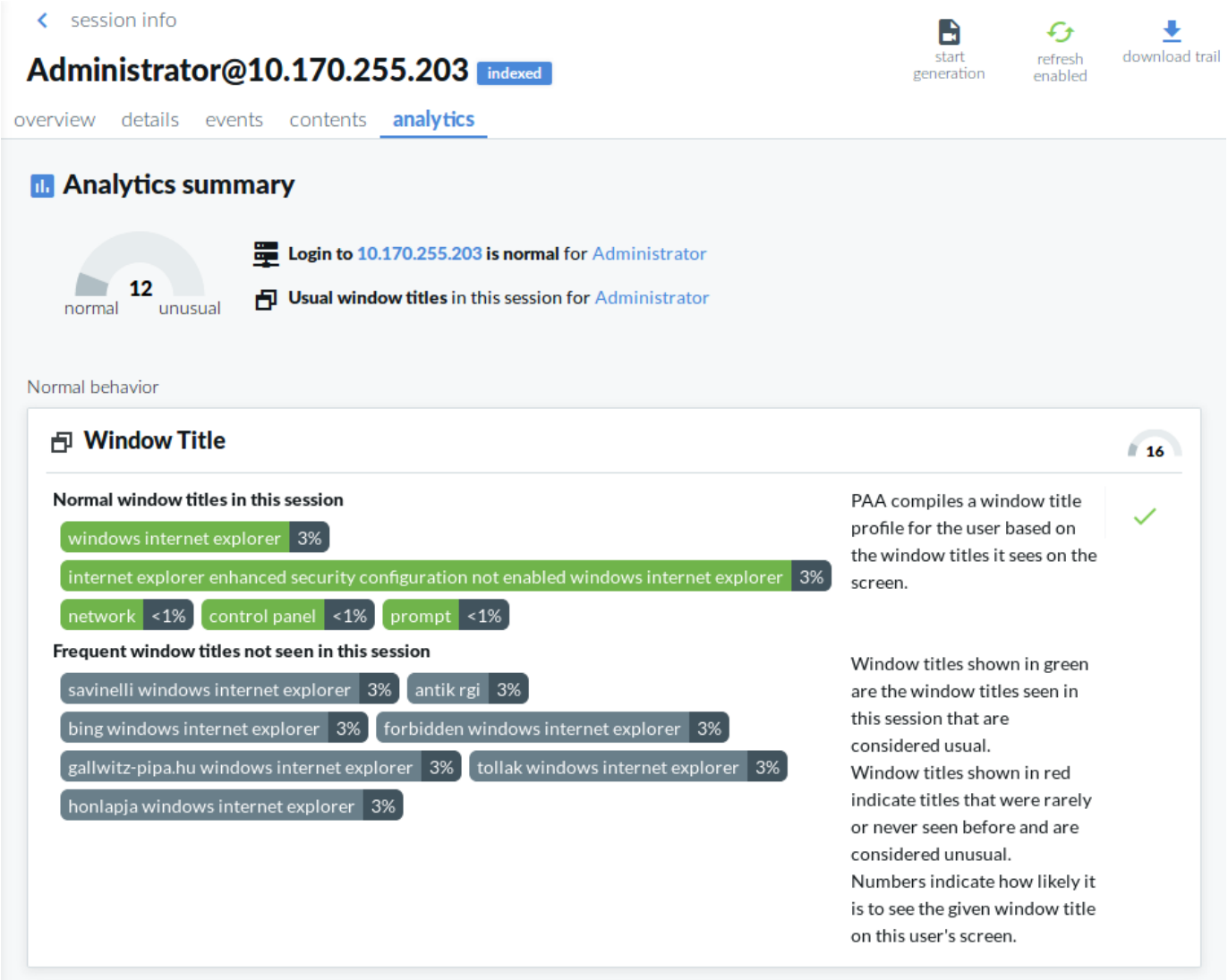


Рис.3.11. Перегляд відомостей на вкладці аналітики: нормальна поведінка

Таким чином привілейована аналітика загроз зменшує шум сповіщень, що створюється SIEM, шляхом класифікації подій користувача на основі рівня ризику та відхилень, а також виділення найбільш підозрілих подій. Сповіщення можна надсилати до SIEM, щоб аналітики з безпеки могли переглядати пріоритетний список подій в інтуїтивно зрозумілому інтерфейсі користувача, що дозволяє їм зосередитися на найважливіших подіях [10, 11].

3.4. Розробка загальних рекомендацій щодо захисту привілейованих даних користувачів

Визначимо загальні рекомендації щодо управління привілейованим доступом для організацій

З усього викладеного можна сказати, що чим більше цілісними будуть політики безпеки та дотримання привілеїв, тим краще можливість реагувати на внутрішні та зовнішні загрози, а також виконувати вимоги відповідності.

Найбільш важливими рекомендації PAM є:

Встановіть та застосуйте політику управління привілеями для визначення порядку надання та скасування привілейованого доступу та облікових записів.

Визначте та візьміть під контроль усі привілейовані облікові записи та дані (бази даних, програми, служби, соцмережі тощо), включаючи ті, що використовуються постачальниками.

Забезпечте найменшу кількість привілеїв для кінцевих користувачів, кінцевих точок, облікових записів, програм, служб, систем тощо.

Застосуйте технологію для підвищення привілеїв, необхідних для виконання певних дій та скасування привілеїв після завершення діяльності.

Підвищуйте привілеї в міру необхідності для конкретних додатків та завдань лише в той момент, коли вони потрібні.

Обмежте кількість привілейованих облікових записів якомога меншою кількістю людей.

Мінімізуйте кількість прав для кожного привілейованого облікового запису.

Кожен привілейований обліковий запис повинен мати точно налаштовані привілеї для виконання певного набору завдань.

Системи та мережі, що вимагають більш високих рівнів довіри, повинні реалізовувати більш надійні засоби контролю безпеки.

Забезпечте надійні паролі, які можуть протистояти поширеним типам атак (наприклад, перебір, на основі словника тощо) і регулярно змінюйте їх.

Для конфіденційних привілейованих доступів використовуйте одноразові паролі.

Використовуйте автентифікацію єдиного входу (SSO), щоб приховати паролі від користувачів та процесів.

Забезпечте доступ з мінімальними привілеями на основі вразливостей, що дозволить вам автоматично обмежувати привілеї та запобігати небезпечним операціям.

Увімкніть базові показники для дій привілейованих користувачів та інші дані про ризики для більшого уявлення про ризики привілеїв.

Основні переваги PAM:

Автоматизовані, попередньо упаковані рішення PAM здатні масштабуватись на мільйони привілейованих облікових записів та активів для підвищення безпеки та відповідності вимогам.

Рішення PAM можуть автоматизувати виявлення, керування та моніторинг, щоб усунути прогалини у привілейованому покритті облікових записів та облікових даних, одночасно оптимізуючи робочі процеси та значно зменшуючи адміністративну складність.

Управління привілейованими доступами допоможе підвищити безпеку за допомогою:

Ведення повного списку всіх активних привілейованих облікових записів у мережі та оновлення цього списку при кожному створенні нового облікового запису.

Зберігання привілейованих ідентифікаторів, таких як паролі, ключі SSH та сертифікати SSL у безпечному сховищі.

Застосування суворих безпекових політик, що охоплюють складність пароля, частоту його скидання, створення надійних пар ключів SSH і так далі.

Надання привілейованого доступу з мінімальними дозволами, необхідні для виконання завдання.

Аудит усіх операцій з ідентифікацією, таких як вхід для привілейованих користувачів, спільні паролі, спроби доступу до пароля, дії скидання тощо.

Моніторинг та запис усіх сеансів привілейованих користувачів у режимі реального часу.

ВИСНОВКИ

В результаті виконання магістерської роботи було отримано наступні наукові результати:

Визначено основні логічні групи рішень доступу до інформаційної системи організації, до яких відноситься ідентифікація, привілеї та активи. Згідно стандартів та рекомендацій було визначено, що для захисту інформаційної системи існують вказівки як забезпечити захист привілейованих даних користувачів. В результаті чого отримано концепцію П’ять А.

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

Проаналізовано загрози та приклади атак для отримання привілейованих даних користувачів інформаційної системи організації, а також міри по їх усуненню.

Проаналізовано та обрано технологію привілейованого захисту користувачів інформаційної системи організації на базі технології One Identity Safeguard, яка займає одне з перших місць в Магічному квадранті Gartner.

Визначено основні модулі та роботу логічних об’єктів, які входять до архітектури системи привілейованого доступу користувачів інформаційної системи організації.

На основі отриманих даних розроблено варіант технології розгортання та налаштування рішення One Identity Safeguard привілейованого захисту користувачів інформаційної системи організації, які до зволять виявляти аномальну поведінку привілейованих користувачів.

В результаті виконання роботи надано рекомендації фахівцям з кібербезпеки щодо захисту привілейованих даних користувачів інформаційної системи організації.

.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. Привієльований доступ [Електронний ресурс] – Режим доступу: https://cloudnetworks.ru/analitika/chto-takoe-pam/

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

4. Привієльовані записи [Електронний ресурс] – Режим доступу: https://www.kv.by/blog/users/softline/1061251-krazha-privilegirovannyh-zapisei-vy-v-bezopasnosti

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

6. Архітектура привілейованого доступу [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/reviews/One-Identity-Safeguard .

7. One Identity Safeguard for Privileged passwords [Електронний ресурс] – Режим доступу: https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.11.1/administration-guide

8. Двофакторна аутентифікація Starling [Електронний ресурс] – Режим доступу: https://support.oneidentity.com/starling-two-factor-authentication/hosted/technical-documents .

9. One Identity Safeguard for Privileged Sessions [Електронний ресурс] – Режим доступу: https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-sessions/6.11.1/administration-guide/2 .

10 One Identity Safeguard for Privileged Analytics [Електронний ресурс] – Режим доступу: https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-

privileged-sessions/6.11.1/safeguard-for-privileged-analytics-configuration-guide/2#TOPIC-1693151

11. One Identity Safeguard for Privileged Analytics. Конфігурація [Електронний ресурс] – Режим доступу: https://support.oneidentity.com/technical-documents/safeguard-for-privileged-sessions/5.8.0/safeguard-for-privileged-analytics-configuration-guide

12. Привілейований доступ [Електронний ресурс] – Режим доступу: https://safe-surf.ru/specialists/article/5280/660532/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)