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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованим доступом в інформаційній системі організації»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микита ВОРОТНЯК
(підпис)

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

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

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

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APM – Application Password Management

CIP – Critical Infrastructure Protection

CPM – Central Policy Manager

DNA – Discovery and Audit

DR Vault – Disaster Recovery Vault

Vault – Digital Vault

ENE – Event Notification Engine

EPM – Endpoint Privilege Manager

EPV – Enterprise Password Vault

EVD – Export Vault Data (Utility)

HA – High Availability

HSM – Hardware Security Module

IAM – Identity and Access Management

IDM – Identity Management

MP – Master Policy

MSSP – Managed (Secure) Service Provider

PA Client – PrivateArk Client

PACLI – PrivateArk Command Line Interface

PAM – Self-Hosted Privileged Access Manager - Self-Hosted

PIM – Privileged Identity Management

PSM – Privileged Session Manager

PTA – Privileged Threat Analytics

PVWA – Password Vault Web Access

SIEM – Security Information and Event Management

ВСТУП

Управління привілейованим доступом (Privileged Access Management, PAM) стає дедалі важливим для сучасних організацій, які прагнуть захистити свої критичні ресурси та конфіденційну інформацію. З розвитком цифрових технологій кількість даних, до яких обмежений доступ, швидко зростає, як і кількість загроз для них. Зловмисники намагаються отримати доступ до привілейованих облікових записів, які надають доступ до найбільш критичних даних організації. Тому ефективне PAM-рішення є основою для контролю доступу до інформаційної системи, що дозволить зменшити ризики від сторонніх атак та внутрішніх інцидентів.

Адміністратори, які спостерігають за користувачами привілейованого доступу, забезпечують прозорий моніторинг привілейованих доступів та керування ними. Це включає відстеження активності користувачів із привілейованими правами, автоматизацію запитів на доступ, а також встановлення обмежень на дії навіть для авторизованих користувачів. Завдяки цій організації можна забезпечити ефективний контроль над тим, хто і коли отримує доступ до критичних ресурсів, що знижує ймовірність витоку даних чи інших кіберзагроз, спричинених несанкціонованими діями чи порушенням політики безпеки.

Слід зазначити, що PAM сприяє дотриманню нормативних вимог, зокрема для організацій у сфері фінансів, охорони здоров'я та урядових установ. Такі вимоги часто передбачають суворий контроль доступу до даних, і PAM надає всі необхідні інструменти для звітності й аудиту. Отже, управління привілейованим доступом є ключовим аспектом сучасної кібербезпеки, який дозволяє знизити ризики безпеки, забезпечити відповідність вимогам регуляторів та підтримувати довіру клієнтів.

Таким чином, кваліфікаційна робота, яка присвячена управлінню привілейованим доступом до інформаційної системи організації відіграє велике значення забезпечення безпеки організацій у сучасному інформаційному середовищі.

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

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

Метою роботи – роботи розробка варіанту технології управління привілейованим доступом в інформаційній системі організації та розробка рекомендації щодо її застосування.

Наукові завдання:

дослідити сутність проблеми управління привілейованим доступом до інформаційної системи організації;

проаналізувати підходи до вирішення проблеми захисту привілейованих користувачів;

проаналізувати існуючі технології управління привілейованим доступом;

проаналізувати методи та засоби управління привілейованим доступом до інформаційної системи організації;

розкрити порядок реалізації технології управління привілейованим доступом на прикладі CyberArk PAM;

надати рекомендації щодо використання CyberArk PAM для управління привілейованим доступом.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління привілейованим доступом CyberArk PAM, а також розроблено рекомендації для фахівців з кібербезпеки щодо застосування даної технології.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз поняття управління привілейованим доступом інформаційної системи організації

«Привілейований доступ» до інформаційної системи організації – це термін, який використовується для визначення спеціального доступу або можливостей, що виходять за рамки стандартного користувача інформаційної системи організації. Привілейований доступ дозволяє організаціям захищати свою інфраструктуру та програми, ефективно вести бізнес і забезпечити конфіденційність, доступність до критичної інфраструктури [1, 2, 13].

Привілейований доступ може бути пов’язаний як з користувачами-людьми, так і з користувачами, які не є людьми, наприклад програмами та ідентифікаторами машин.

До привілейованого доступу, який використовують спеціальні користувачі інформаційної системи відноситься:

Обліковий запис суперкористувача. Обліковий запис суперкористувача представляє собою спеціальний обліковий запис, який використовується адміністраторами IT-системи, який використовується для налаштування системи чи програми, додавання чи видалення звичайних користувачів або видалення даних [1, 2].

Обліковий запис адміністратора домену. Такий обліковий запис, надає привілейований адміністративний доступ до всіх робочих станцій і серверів у мережевому домені. Цих облікових записів зазвичай небагато, але вони забезпечують найрозширеніший і надійний доступ у всієї інфраструктури організації [1, 2].

Обліковий запис локального адміністратора. Цей обліковий запис розташований на кінцевій точці або робочій станції та використовує комбінацію

імені користувача та пароля. Це допомагає людям отримувати доступ до своїх локальних машин або пристроїв і вносити зміни в них [1, 2].

Ключ SSH (Secure Socket Shell). Ключі SSH – це широко використовувані протоколи контролю доступу, які надають прямий кореневий доступ до критично важливих систем. Корінь — це ім'я користувача або обліковий запис, який за умовчанням має доступ до всіх команд і файлів у Linux або іншій Unix-подібній операційній системі [1, 2].

Екстрений обліковий запис. цей обліковий запис надає користувачам адміністративний доступ до захищених систем у разі надзвичайної ситуації. Його іноді називають обліковим записом пожежного виклику або розбиття скла [1, 2].

Привілейований бізнес-користувач. До цього виду привілейованого доступу відноситься хтось, хто працює поза IT, але має доступ до конфіденційних даних інформаційної системи. Це може включати когось, кому потрібен доступ до фінансів, людських ресурсів (HR) або маркетингових систем [1, 2].

Привілейований доступ який використовується не людьми, а процесами які запускають важливі процеси в інформаційній системі організації часто називають нелюдським привілейованим доступом. До такого доступу відноситься:

Обліковий запис програми. привілейований обліковий запис, який є специфічним для прикладного програмного забезпечення та зазвичай використовується для адміністрування, налаштування або керування доступом до прикладного програмного забезпечення [1, 2].

Обліковий запис служби. Обліковий запис, який програма або служба використовує для взаємодії з операційною системою. Служби використовують ці облікові записи для доступу та внесення змін до операційної системи чи конфігурації системи [1, 2].

Ключ SSH. Ключі SSH також використовуються автоматизованими процесами [1, 2].

Секрет. Часто використовується групою розробки та операцій (DevOps) як загальний термін, що стосується ключів SSH, ключів інтерфейсу прикладної

програми (API) та інших облікових даних, які використовуються командами DevOps для надання привілейованого доступу [1, 2].

Привілейовані облікові записи, облікові дані та секрети існують скрізь: за оцінками фахівців, вони можуть перевищують кількість співробітників організації у три-чотири рази. У сучасних бізнес-середовищах поверхня атак, пов’язаних із привілеями, швидко зростає, оскільки системи, програми, міжмашинні облікові записи, хмарні та гібридні середовища, DevOps , роботизована автоматизація процесів і пристрої IoT стають все більш взаємопов’язаними. Зловмисники це знають і націлюються на привілейований доступ. У разі зловживання привілейованим доступом можна порушити бізнес-процеси всієї організації.

Рішення PAM ідентифікує людей, процеси та технології, яким потрібний привілейований доступ та вказує, які політики необхідно до них застосувати. Рішення PAM має підтримувати встановлені вами політики (наприклад, автоматичне керування паролями та багатофакторну автентифікацію), а у адміністраторів повинна бути можливість автоматизувати процес створення, зміни та видалення облікових записів. Крім того, рішення PAM має постійно відстежувати сеанси, щоб ви могли створювати звіти для виявлення та дослідження аномалій.

Отже, Privileged Access Management використовується для запобігання витоку інформації через облікові дані та забезпечення відповідності вимогам.

Викрадення привілейованих облікових записів – це крадіжка злочинцем даних для входу з метою отримання доступу до облікового запису користувача. Після входу в систему зловмиснику стають доступними дані організації. Він може встановити шкідливі програми на різні пристрої, а також отримати доступ до систем вищого рівня. Технологія PAM дозволяє локалізувати ризик, оскільки доступ надається лише у потрібний час, тільки з необхідними привілеями та лише за умови багатофакторної перевірки автентичності всіх облікових записів адміністраторів [13].

Рішення PAM можна використовувати для автоматизації життєвого циклу користувачів (наприклад, для створення, підготовки та відкликання облікових записів), моніторингу та реєстрації привілейованих облікових записів, безпечного віддаленого доступу та управління доступом зовні. Рішення PAM можна також застосовувати до пристроїв (Інтернет речей), у хмарних середовищах та проектах DevOps.

Зловживання привілейованими обліковими записами спричиняє загрозу кібербезпеці, здатну завдати великої та істотної шкоди організації. Рішення PAM має потужні функції, що дозволяють ефективно усувати ризики.

1.2. Аналіз загроз привілейованому доступу до інформаційної системи організації

Атака з підвищенням привілеїв — це кібератака з метою отримання незаконного доступу до підвищених прав, дозволів, повноважень або привілеїв, які перевищують ті, що призначені для особи, облікового запису, користувача або машини. Ця атака може включати зовнішню загрозу або внутрішню загрозу. Ескалація привілеїв є ключовим етапом ланцюжка кібератак і зазвичай передбачає використання вразливості ескалації привілеїв, такої як системна помилка, неправильна конфігурація або невідповідний контроль доступу.

Розглянемо, як працює ескалація привілеїв, ключові вектори атак, пов’язані з ескалацією привілеїв, і критично важливі елементи керування безпекою привілейованого доступу, які можна застосувати, щоб запобігти або пом’якшити це.

Кожен локальний інтерактивний сеанс або сеанс віддаленого доступу представляє певну форму привілейованого доступу, незалежно від того, виконується людиною чи машиною. Це охоплює все: від привілеїв гостя, які дозволяють лише локальний вхід, до прав адміністратора або root для віддаленого сеансу та потенційно повного контролю над системою. Таким чином, кожен обліковий запис, який взаємодіє з системою, має певні привілеї [3, 13].

Обліковий запис стандартного користувача рідко має права доступу до бази даних, конфіденційних файлів чи щось цінного. Отже, зловмисник який отримує привілейований доступ до інформаційної системи орієнтується в середовищі та отримує права адміністратора або root і може використовувати їх як вектор атаки. Є п'ять основних методів отримання привілейованого доступу [3]:

– використання облікових даних;
– уразливості та експлойти;
– неправильні конфігурації;
– шкідливе програмне забезпечення;
– соціальна інженерія.

На рис.1.1. наведено діаграму ланцюжка атак, яка показує основні методи, які застосовує зловмисник, незалежно від того, внутрішня чи зовнішня загроза, для початку своєї місії та поширення в середовищі.

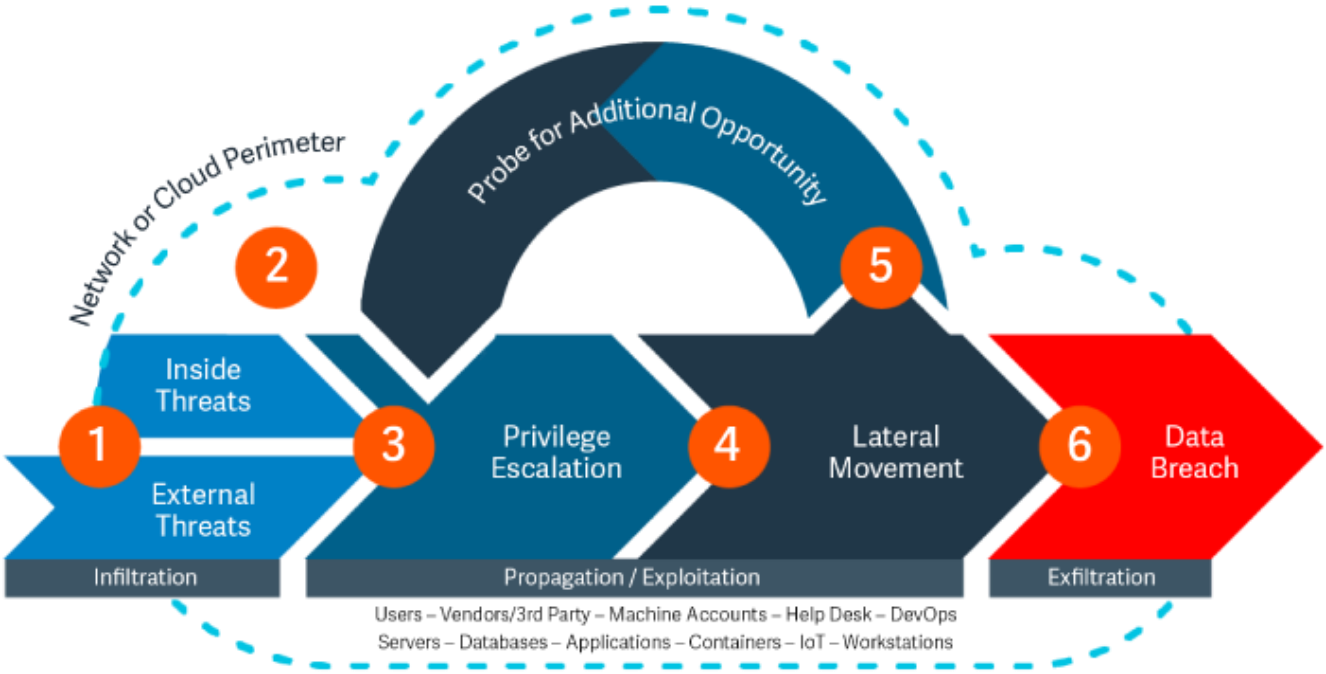


Рис.1.1. Вектор атак на підвищення привілеїв

Атаки на підвищення привілеїв починаються з того, що суб'єкти загроз проникають у середовище. Зловмисник може закріпитися, використовуючи відсутні патчі безпеки, соціальну інженерію або інші методи, починаючи від базового підбору пароля (або введення облікових даних) і закінчуючи сучасними

методами з використанням генеративного штучного інтелекту. Після успішного початкового проникнення загрозливі суб’єкти зазвичай здійснюють спостереження та чекають відповідної нагоди, щоб продовжити свою місію.

Суб’єкти загроз прагнуть йти шляхом найменшого опору. Якщо дозволяє час, вони прибирають свою діяльність, щоб залишатися непоміченими. Незалежно від того, чи це стосується маскування їхньої вихідної IP-адреси чи видалення журналів на основі облікових даних, які вони використовують, будь-які докази їх присутності відображають індикатор компрометації (IoC). Щойно організація ідентифікує вторгнення, вона може контролювати наміри зловмисника та потенційно призупинити або припинити сеанс доступу.

Як правило, другий крок у ланцюжку кібератак включає ескалацію привілеїв до облікових записів із адміністраторськими правами, правами root або вищими привілеями, ніж той обліковий запис, який був зламаний. Звичайно, можливо, початкова компрометація включає обліковий запис адміністратора або root. Якщо це так, зловмисникще більше просувається у своїх зловмисних планах і, можливо, вже має доступ до середовища.

Вертикальна та горизонтальна ескалація привілеїв

Атаки на підвищення привілеїв поділяються на дві великі категорії — горизонтальне підвищення привілеїв і вертикальне підвищення привілеїв.

Ці терміни, які часто плутають один з одним, визначаються наступним чином:

Горизонтальна ескалація привілеїв

Горизонтальна ескалація привілеїв включає отримання доступу до прав іншого облікового запису — людини чи машини — з подібними привілеями. Ця дія називається «захопленням облікового запису». Як правило, це стосуватиметься облікових записів нижчого рівня (тобто стандартного користувача), які можуть не мати належного захисту. З кожним новим скомпрометованим горизонтальним обліковим записом зловмисник розширює свою сферу доступу зі схожими привілеями. Це основний бічний рух.

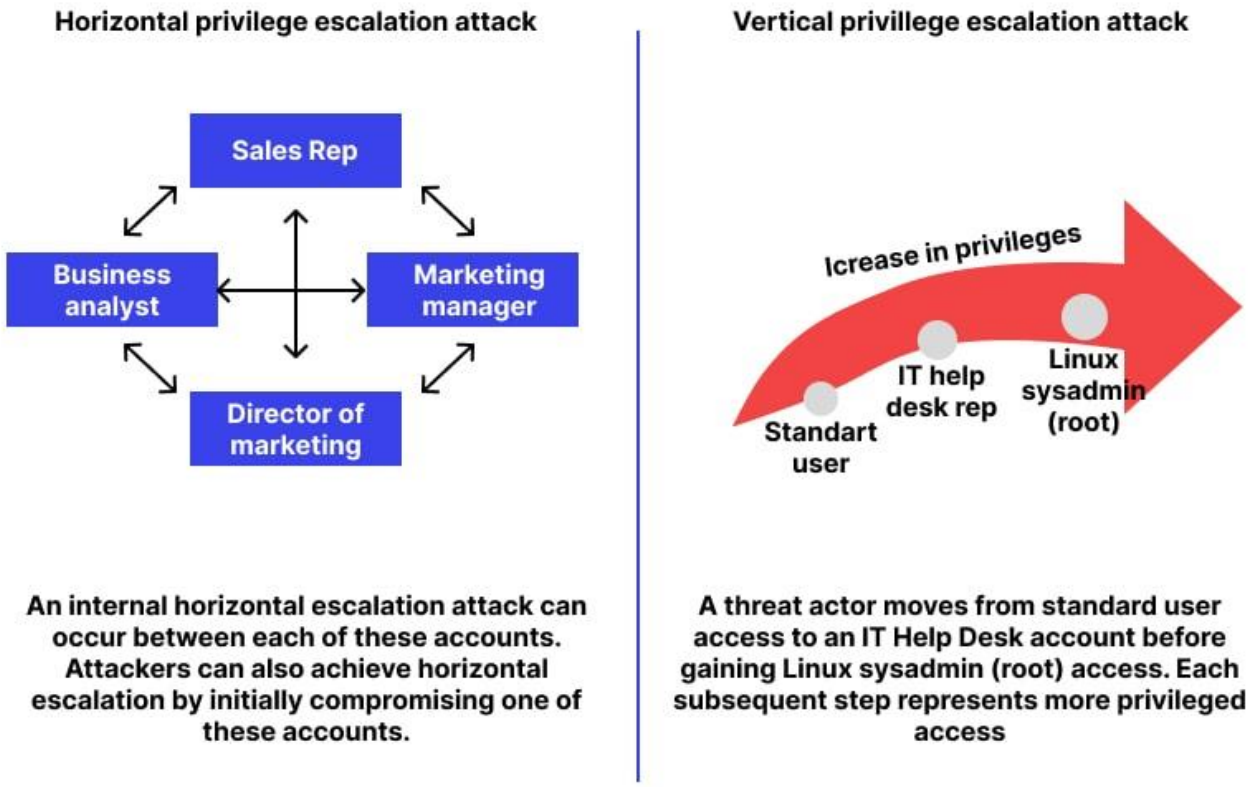


Рис.1.2. Вертикальна та горизонтальна ескалація привілеїв [4]

Вертикальна ескалація привілеїв

Вертикальна ескалація привілеїв , також відома як атака на підвищення привілеїв, передбачає збільшення привілеїв/привілейованого доступу понад те, що вже має користувач, програма чи інший ресурс. Це передбачає перехід від низького рівня привілейованого доступу до вищого рівня привілейованого доступу. Досягнення вертикальної ескалації привілеїв може вимагати від зловмисника виконання ряду проміжних кроків (наприклад, виконання атаки переповнення буфера тощо), щоб обійти або скасувати контроль привілеїв або використати недоліки програмного забезпечення, мікропрограми, ядра або отримати привілейовані облікові дані для інші програми або сама операційна система.

Основні ключові стратегії нападу, які агресори використовують для завершення ескалації привілеїв полягають у наступному.

1. Соціальна інженерія

По суті, кожна кібератака використовує соціальну інженерію . Зловмисники часто використовують цю стратегію, щоб отримати несанкціонований доступ і збільшити привілеї [4].

Оскільки соціальна інженерія є надзвичайно успішною і обходить засоби безпеки безпеки, переслідуючи слабкі місця людей. Зловмисники знають, що обійти захищену систему кіберзахисту значно простіше, якщо задіяний улюблений клієнт.

Найпоширеніші типи атак соціальної інженерії та способи їх застосування для підвищення привілеїв:

Фішинг — це коли програміст повідомляє щось конкретне, що виглядає справжнім, але містить зловмисне вкладення. Зловмисник, як правило, використовує шкідливе програмне забезпечення для проникнення в гаджет жертви, якщо він натискає з'єднання або відкриває його. За умови зараження нападник може отримати доступ до облікових даних клієнта.

Skewer phishing — це сучасний фішинг, вирощений виключно для улюбленої особи або групи клієнтів. Наприклад, зловмисники можуть використовувати флеш-фішинг, щоб отримати доступ до дуже привілейованих облікових записів, як-от облікових записів директорів фреймворку, банківських працівників або вищих керівників.

Scareware — це оманливе програмне забезпечення, яке змушує клієнтів думати, що їхні гаджети заражені, а потім просить їх завантажити інше програмне забезпечення або зробити крок, заражаючи їхні ПК шкідливим програмним забезпеченням. Гаджет жертви може бути взломано, і його дані скомпроментовано.

Фармінгом відбувається, коли зловмисне програмне забезпечення, запроваджене на гаджеті жертви, спрямовує його на фальшивий сайт, який імітує дійсний, як-от банк чи офіційний сайт компанії. Жертву обманюють, щоб вона відкрила конфіденційні дані, які зловмисник може використати, щоб отримати доступ до його запису.

2. Використання облікових даних

Зловмисники, які сподіваються підвищити свої привілеї, мають вхід із однофакторною автентифікацією. Дійсно, навіть без секретної фрази нападники можуть зрештою отримати секретне слово, якщо вони дізнаються записне ім’я необхідного клієнта. Вони можуть непомітно перевіряти дані, коли мають законну секретну фразу.

Далі йдуть регулярні стратегії, за допомогою яких агресори можуть отримати доступ:

Розкриття пароля: працівники зазвичай повторно використовують, поширюють або зберігають свої паролі у вигляді відкритого тексту на своїх комп’ютерах, показуючи їх для загального огляду.

Спроба ввести пароль: щоб зробити обґрунтовані висновки щодо секретного слова, зловмисники можуть використовувати дані про власника запису, які є у вільному доступі. Крім того, оскільки паролі регулярно використовуються повторно, зловмисники, які порушують одну секретну фразу, можуть діставатися до різних активів.

Перегляд з-за плеча: це дія агресора, який спостерігає за подіями особи в довіреному місці, або безпосередньо, або за допомогою клавіатурних шпигунів, запроваджених на пристроях.

Словникові атаки: атака, під час якої потенційні паролі консолідуються та використовуються для отримання доступу до облікового запису з використанням звичайних термінів. Зловмисники можуть налаштувати посилання на слово, щоб відповідати відомим секретним вимогам і довжині фрази. Цим атакам можна запобігти, використовуючи секретні ключові стратегії складності та секретні обмеження повторних спроб.

Груба сила: щоб досягти успіху, зловмисники намагаються застосувати пароль грубою силою, якщо нічого не допомагає. Можливо, вони функціонують, коли кількість повторних спроб секретної фрази необмежена, а паролі короткі та нескладні.

Розпорошення пароля: на відміну від атаки грубою силою, розпилення пароля включає комп’ютеризовану роботу для доступу до незліченних записів за допомогою кількох добре відомих паролів.

Передача облікових даних : це коли зловмисник намагається отримати доступ до облікових записів на об’єктивній основі, використовуючи набір імен користувачів, адрес електронної пошти та паролів, які він отримав від попередніх хакерів або темної мережі. Ця стратегія є дуже потужною, оскільки паролі часто використовуються повторно.

Оновлення та скидання секретних слів: системи для скидання таємних слів безпорадні проти атак. Зловмисники можуть отримати доступ до секретного слова, яке клієнт законно змінив, або вони можуть запросити змінити свій секретний ключ після зламу гаджета [3, 4].

3. Неправильні конфігурації

Неправильна конфігурація, грубі помилки в налаштуванні брандмауера або відкриті порти, часто спонукають до підвищення привілеїв.

Кілька випадків грубих помилок безпеки, які можуть призвести до ескалації привілеїв, наведені нижче.

Стандартні паролі для облікових записів root або адміністратора (це нормально для гаджетів IoT) [3, 4].

4. Уразливості та експлойти

Використовуючи недоліки у створенні, виконанні або налаштуванні кількох систем, наприклад, протоколів зв’язку, комунікаційних транспортів, операційних систем, програм, веб-додатків, хмарних адміністраторів і організаційних основ, зловмисники можуть підвищити свої привілеї.

Визначення рівня ризику залежить від стану дефекту та того, наскільки важливим для системи є виявлення слабкого місця. Вертикальна ескалація привілеїв можлива лише за невеликого рівня недоліків [3, 4].

5. Шкідливе програмне забезпечення

Зловмисне програмне забезпечення , як-от трояни, шпигунське програмне забезпечення, хробаки та програми-вимагачі, можуть використовуватися

зловмисниками, щоб утримати контроль і повну ескалацію привілеїв. Зловмисне програмне забезпечення можна поширювати, використовуючи слабкі місця, шкідливими з'єднаннями чи завантаженнями, поєднаними з соціальною інженерією, або користуючись недосконалістю робочої мережі.

До такого шкідливого програмного забезпечення відносяться:

Хробаки — це зловмисне програмне забезпечення, яке поширюється на різні комп'ютери, використовуючи недоліки та слабкі місця для передачі руйнівного корисного навантаження. Хробаки — це поширена стратегія для підвищення привілеїв на рівні рівня.

Руткіти — це проекти, запроваджені на необхідному гаджеті, які надають злавмиснику повний доступ до його робочої структури, надаючи йому напрямок угору для підвищення своїх привілеїв.

Боти — це механізовані пристрої, на яких зосереджені зловмисники, виконуючи деструктивну діяльність. Наприклад, боти зазвичай використовуються для надсилання хробаків і можуть використовуватися на етапі спостереження атаки з підвищенням привілеїв.

Троян - зловмисне програмне забезпечення імітує справжній документ або програму, залишається на гаджеті клієнта та може запроваджувати більше зловмисного програмного забезпечення та змінювати налаштування фреймворку. Багато нападів, які використовують автентифікацію, залежать від троянів.

Рекламне ПЗ - це різновид шкідливого ПЗ, яка показує клієнтам небажану рекламу. Коли ці оголошення співпрацюють, на гаджет може бути введено додаткове зловмисне програмне забезпечення, яке працює як метод підвищення привілеїв.

Шпигунське програмне забезпечення - використовується, щоб стежити за гаджетом, наприклад, відстежуючи натискання клавіш клієнтом або доступ до екрана, приймача чи камери. Крім того, зловмисники можуть проникати в записи клієнтів і отримувати сертифікати, використовуючи ці джерела інформації [3, 4].

1.3. Підходи організації привілейованого доступу до інформаційної системи організацій

Оскільки атаки на підвищення привілеїв можуть починатися та розвиватися безліччю різних способів, для захисту потрібні численні стратегії та тактики захисту. Однак впровадження підходу, орієнтованого на ідентифікацію, і засобів керування привілейованим доступом допоможе вашій організації захиститися від найширшого спектру атак і досягти максимального зменшення площі атак. Розглянмо основні підходи до організацій, які хочуть впровадити заходи та методи захисту привілейованого доступу.

Повністю керуйте життєвим циклом ідентифікації користувачів, включаючи надання та скасування ініціалізації ідентифікаторів і облікових записів, щоб переконатися, що немає загублених облікових записів для викрадення.

Впроваджувати технології з рішенням для керування паролями, щоб послідовно застосовувати надійні практики керування обліковими даними (виявлення, зберігання, централізоване керування, реєстрація, виписка) як для людей, так і для машин. Це також тягне за собою усунення стандартних і жорстко закодованих облікових даних.

Застосувати мінімальні привілеї. Позбавити користувачів прав адміністратора та зменшити привілеї програм і комп’ютера до необхідного мінімуму. Необхідно також реалізувати своєчасний доступ, щоб зменшити постійні або постійні привілеї.

Впроваджувати розширений контроль і захист додатків, щоб забезпечити детальний контроль над усіма доступами додатків, зв’язками та спробами підвищення привілеїв.

Відстежувати та керувати всіма привілейованими сеансами, щоб виявити та швидко усунути будь-яку підозрілу активність, яка може свідчити про викрадений обліковий запис або незаконну спробу ескалації привілеїв або бічне переміщення.

Впровадити заходи та методи щодо зміцнення систем і програм. Це доповнює принцип найменших привілеїв і може передбачати зміни конфігурації, видалення непотрібних прав і доступу, закриття портів тощо. Це покращує безпеку системи та додатків, а також допомагає запобігти й пом'якшити ймовірність помилок, які створюють вразливість до ін'єкцій шкідливого коду (наприклад, ін'єкцій SQL), переповнення буфера тощо або інших бекдорів, які можуть дозволити ескалацію привілеїв.

Впроваджуйте методи керування вразливими місцями. Постійно виявляйте та виправляйте вразливі місця, наприклад, виправляючи неправильні конфігурації, усуваючи стандартні та/або вбудовані облікові дані тощо.

Використовувати захищений віддалений доступ. Завжди слід контролювати та керувати для будь-якої форми привілейованого доступу, оскільки атаки можуть відбуватися горизонтально та вертикально з метою використання привілеїв.

1.4. Аналіз технологій привілейованого доступу до інформаційної системи організації

Сьогодні на ринку представлено багато рішень, які пропонують технологію управління привілейованим доступом до інформаційної системи організації (рис.1.3). Дослідження Gartner визначає керування привілейованим доступом (PAM) як технології, які забезпечують підвищений рівень технічного доступу через керування та захист облікових записів, облікових даних і команд, які використовуються для адміністрування або налаштування систем і програм [5].

Керування привілейованим доступом (PAM) або керування привілейованим обліковим записом — це процес призначення, моніторингу та захисту доступу до критичних бізнес-систем і програм.

Завдання: привілейовані облікові записи мають вищий рівень доступу до критично важливих систем, які містять конфіденційні або цінні бізнес-дані. Коли зловмисники викрадають або зламують облікові дані для входу в обліковий запис

привілейованого користувача, вони можуть отримати доступ до всіх конфіденційних даних, доступних законному користувачеві.

Рис.1.3. Лідери ринку PAM

Як працює PAM: рішення PAM дозволяють IT-адміністраторам і адміністраторам безпеки контролювати та захищати доступ до критично важливих систем, дозволяючи їм надавати підвищені привілеї «точно вчасно», тобто лише до тих пір, поки вони потрібні користувачеві для виконання своєї роботи. Коли користувач виходить із системи, привілеї скасовуються.

Найкращі рішення PAM, розроблені для захисту критично важливих бізнес-систем від несанкціонованого доступу опишемо з огляду:

Відмінні особливості кожного рішення;

Кому вони найкраще підходять.

З лідерів можна визначити наступні рішення, які використовують технологію PAM:

1. ARCON | Privileged Access Management
2. BeyondTrust Privileged Remote Access
1. Broadcom Symantec Privileged Access Management (PAM)
2. CyberArk Privileged Access Management
3. Delinea Secret Server
4. ManageEngine PAM360
5. Saviynt Cloud PAM
6. One Identity Safeguard

ARCON Керування привілейованим доступом

ARCON PAM дозволяє групам безпеки підприємства захищати та керувати всім життєвим циклом своїх привілейованих облікових записів.

Як це працює: ARCON PAM має безпечне сховище паролів, яке генерує та зберігає надійні динамічні паролі, доступ до яких мають лише авторизовані користувачі. Користувачі повинні підтвердити свою особу за допомогою багатофакторної автентифікації (MFA), щоб отримати доступ до сховища, а привілейовані облікові дані автоматично змінюються між сеансами, усуваючи можливість передачі або викрадення паролів.

Для кого це: ARCON пропонує цілодобову підтримку всім своїм клієнтам як базову пропозицію підтримки, і вони не роблять різниці між рівнями технічної підтримки. Їх рішення PAM також має високу масштабованість. З цих причин ми рекомендуємо ARCON |, хоча використовуємо технологію корпоративного рівня PAM для організації будь-якого розміру, яка шукає надійне рішення PAM.

Переваги: увесь привілейований доступ надається своєчасно; це зменшує поверхню загрози, віддаючи перевагу доступу за потреби над постійними привілеями.

Сховище паролів ARCON, захищене MFA, автоматизує часті зміни паролів, генерує та зберігає надійні динамічні паролі, надаючи користувачам своєчасний

доступ до критично важливих систем без необхідності ділитися своїми обліковими даними.

Платформа використовує власну програмну перевірку одноразового пароля (OTP) для перевірки ідентичності користувачів за допомогою єдиного входу (SSO).

Розширений моніторинг сеансів дає вам повне уявлення про дії привілейованого облікового запису, а механізм звітності платформи забезпечує повний журнал аудиту привілейованих дій із вбудованою аналітикою.

Ціноутворення: інформацію про ціни можна отримати в ARCON за запитом.

Підсумок: ARCON PAM дозволяє захистити та керувати всім життєвим циклом привілейованих облікових записів вашої компанії. Він забезпечує повний захист від інсайдерських атак і порушень облікових даних [6].

Привілейований віддалений доступ BeyondTrust

Привілейований віддалений доступ BeyondTrust дозволяє користувачам керувати внутрішнім і стороннім віддаленим привілейованим доступом і перевіряти його без необхідності використання VPN.

Як це працює: привілейований віддалений доступ зберігає паролі в захищеному хмарному сховищі на пристрої або в BeyondTrust Password Safe. Потім він безпечно вводить облікові дані зі сховища безпосередньо в сеанс.

Для кого це: це рішення для організацій із віддаленими працівниками, яким потрібен доступ до привілейованих систем. Завдяки широкому спектру варіантів розгортання та інсталяції привілейовані користувачі можуть отримати віддалений доступ до критично важливих систем, а адміністратори можуть схвалити або заборонити доступ з будь-якого місця та в будь-який час.

Переваги: функції ін’єкції облікових даних BeyondTrust дозволяють платформі вводити облікові дані зі сховища безпосередньо в сеанс, тобто користувачі не відкривають облікові дані в будь-який момент під час входу.

Ви можете зберігати привілейовані облікові дані в безпечному хмарному сховищі на пристрої або інтегрувати платформу з BeyondTrust Password Safe.

Потужні можливості моніторингу BeyondTrust із журналами аудиту та аналітикою сеансів дають вам точне бачення привілейованої діяльності.

Платформа пропонує настільні консолі для Windows, Mac і Linux, а також веб-консоль і мобільний додаток. За допомогою цих інтерфейсів ви можете віддалено схвалювати запити на доступ і контролювати використання привілейованого облікового запису.

Ціноутворення: інформацію про ціни можна отримати в BeyondTrust за запитом.

Підсумок: привілейований віддалений доступ BeyondTrust забезпечує ефективність роботи співробітників, незалежно від їхнього місцезнаходження, водночас не даючи зловмисникам отримати доступ до критично важливих бізнес-систем [6].

Broadcom Symantec Privileged Access Management (PAM)

Symantec Privileged Access Management (PAM) допомагає організаціям легше відстежувати та керувати доступом до корпоративних облікових записів високого рівня, щоб зменшити ризик порушення облікових даних і забезпечити відповідність галузевим стандартам.

Як це працює: Symantec PAM зберігає привілейовані облікові дані в зашифрованому сховищі, до якого користувачі можуть отримати доступ лише після підтвердження своєї особи. Після входу користувача платформа записує його сеанс, оцінює ризик і запускає автоматичні дії з пом’якшення, якщо виявляє будь-яку аномальну або небезпечну поведінку.

Для кого це: Symantec PAM підходить для великих підприємств, які прагнуть запобігти витоку облікових даних і стороннім атакам компрометації облікових записів. Платформа також добре підходить для підприємств, які вже використовують інші технології безпеки Broadcom/Symantec.

Що нам подобається: цей інструмент не лише дає змогу захистити облікові записи користувачів за допомогою профілактичних заходів, але також дає змогу реагувати на порушення, якщо вони трапляються, за допомогою вбудованої поведінкової аналітики та автоматизованих робочих процесів усунення.

У сховищі Symantec, захищеному 2FA, зберігаються всі привілейовані облікові дані, включаючи паролі користувача та адміністратора, а також ключі SSH.

Безперервний моніторинг активності платформи на основі ML дає змогу порівнювати поточні дії з поведінкою в минулому, щоб виявити підозрілу або аномальну поведінку. Він також пропонує автоматичні варіанти виправлення у разі виявлення підозрілої поведінки.

Ви можете отримати доступ до повних даних аудиту, отриманих під час кожного сеансу, включаючи відеозаписи. Ці дані надійно зберігаються в зашифрованій базі даних.

Ціноутворення: інформацію про ціни можна отримати від партнерів і дистриб'юторів Broadcom за запитом.

Підсумок: Symantec PAM — це повнофункціональне рішення PAM, яке дає змогу не лише контролювати доступ до облікових записів, але й пом'якшувати будь-яку зловмисну активність, що відбувається після входу користувачів, завдяки надійній криміналістиці сеансів, можливостям запису та автоматизації. варіанти рекультивації [6].

Керування привілейованим доступом CyberArk

CyberArk Privilege Access Manager забезпечує багаторівневий захист доступу для привілейованих облікових записів, дозволяючи IT-командам захищати, керувати та записувати дії привілейованих облікових записів.

Як це працює: CyberArk ізолює всі привілейовані облікові дані в безпечному сховищі, допомагаючи запобігти розкриттю облікових даних. Він безперервно сканує мережу, щоб виявити привілейований доступ, а потім дає змогу підтвердити або припинити спроби доступу.

Для кого це: з варіантами локального, хмарного та SaaS розгортання це хороший варіант для будь-якого підприємства, яке шукає надійне, гнучке рішення PAM із сильним фокусом на моніторингу сеансів і виправленні.

Що нам подобається: це рішення чудово запобігає повторним атакам. Якщо виявлено підозрілу поведінку, він припиняє сеанс і автоматично змінює облікові

дані облікового запису, гарантуючи, що зловмисники або скомпрометовані облікові записи не зможуть повторно отримати доступ до системи.

Платформа дозволяє визначити використання привілейованих облікових записів і усунути ризик постійних привілеїв шляхом постійного сканування мережі для виявлення привілейованого доступу. Потім він або додає спроби доступу до черги для перегляду, або автоматично змінює облікові записи та облікові дані на основі ваших політик.

Ви можете отримати доступ до повного відтворення відео та моніторингу натискань клавіш для кожного привілейованого сеансу. Усі записи зберігаються в зашифрованому сховищі.

CyberArk автоматично припиняє привілейовані сесії на основі рівня ризику виявленої поведінки.

Ціноутворення: CyberArk PAM доступний як самостійне рішення від 112 доларів США за користувача або як рішення SaaS на ринку Azure від 17 800,00 доларів США за одноразовий платіж за 1 рік.

Підсумок: PAM-рішення CyberArk забезпечує багаторівневий захист доступу для привілейованих облікових записів. Його централізоване керування та звітування дають вам чітке уявлення про те, хто і чому отримує доступ до критично важливих систем.

CyberArk займає одну з найбільших часток ринку PAM, пропонуючи керовані політикою рішення корпоративного рівня, які дозволяють IT-командам захищати, керувати та записувати дії привілейованих облікових записів [6].

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Архітектура платформи платформи CyberArk

Платформа CyberArk призначена для захисту привілейованого доступу та поєднує потужну інфраструктуру з основними продуктами для надання найбільш комплексного рішення.

Основою інфраструктури є: ізольоване сховище даних, майстер управління політиками, механізм виявлення для визначення змін у локальних та хмарних IT-середовищах. Компоненти інфраструктури забезпечують масштабованість, надійність та повний захист привілейованого доступу. Гнучка архітектура може починатися з малих розгортань і масштабувати до найбільших та ресурсомістких корпоративних розмірів.

Платформа CyberArk надає рішення, які дозволяють комплексно захищати, контролювати та перевіряти облікові дані користувачів та програм, надавати доступ з мінімальними привілеями, а також керувати програмами на кінцевих точках та серверах. Рішення CyberArk забезпечують захист, моніторинг та аналіз усієї привілейованої активності з активним оповіщенням про аномальну поведінку.

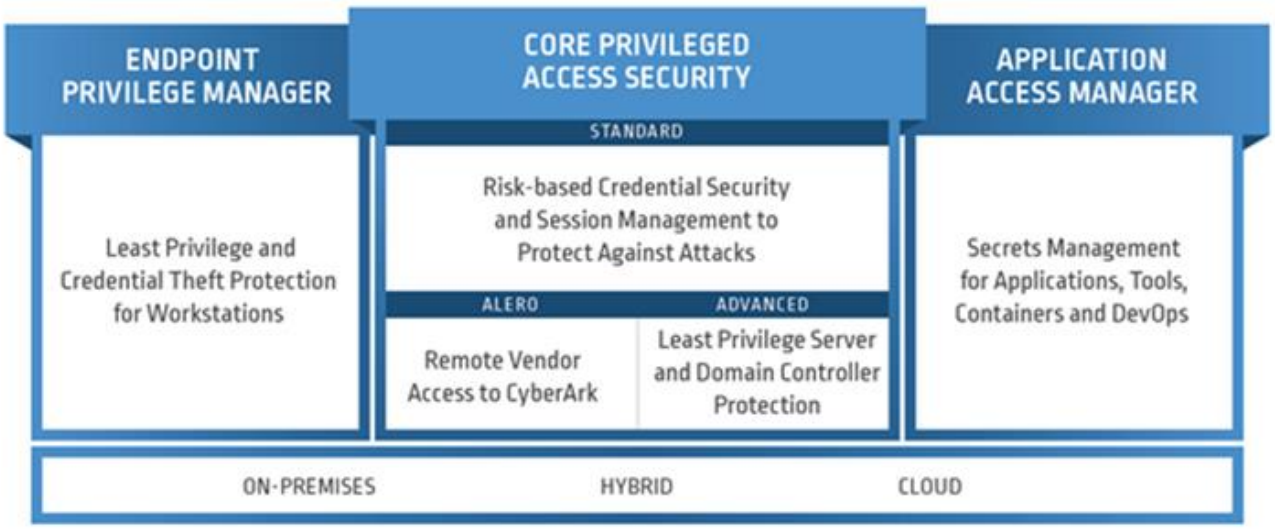


Рис.2.1. Архітектура платформи CyberArk

Основою платформи CyberArk є три основних компонента: Endpoint privilege manager, Application access manager, Core Privileged access security.

1. Endpoint privilege manager надає мінімальні привілеї та захист від крадіжки облікових даних на робочих станціях.

2. Application access manager -дозволяє управління секретами для додатків, інструментів, контейнерів та DevOps.

3. Core Privileged access security

– забезпечує безпеку облікових даних та керування сеансами з урахуванням ризиків для захисту від атак.

– надає доступ віддаленим постачальникам до платформи CyberArk.

– надає мінімальні привілеї на серверах та захист контролерів домену.

Механізм виявленняпривілейв, призначений для постійного виявлення змін у локальних або хмарних IT-середах, забезпечує постійну актуальність захисту, а також реєстрацію та безпеку всієї привілейованої активності. При додаванні або видаленні серверів і робочих станцій всі зміни в привілейованих облікових записах з'являються в автоматичному режимі.

Рішення CyberArk Privileged Access Security забезпечує автоматизоване застосування політики щодо привілейованих облікових записів, що дозволяє безперервно контролювати дотримання вимог аудиту. Фахівці з IT-аудиту отримують повне представлення про те, «ким, коли і чому», а також «що» саме відбувалося під час усіх привілейованих сеансах. Рішення дозволяє зручно й економічно ефективно надавати звіти про результати аудиту через єдиний централізований репозиторій усіх контрольних даних.

2.1. Компоненти архітектури рішення безпеки привілейованого доступу

Архітектура рішення безпеки привілейованого доступу складається з двох основних елементів. Одним з них є Storage Engine (який також називають «сервером» або просто «сховищем»), який зберігає дані та відповідає за безпеку

даних у стані спокою та забезпечення автентифікованого та контрольованого доступу.

Другим елементом є інтерфейс (інтерфейси Windows, веб-інтерфейси та пакети SDK), який взаємодіє з системою зберігання, з одного боку, і надає доступ користувачам і програмам, з іншого. Storage Engine та інтерфейс взаємодіють за допомогою безпечного протоколу CyberArk – протоколу Vault.

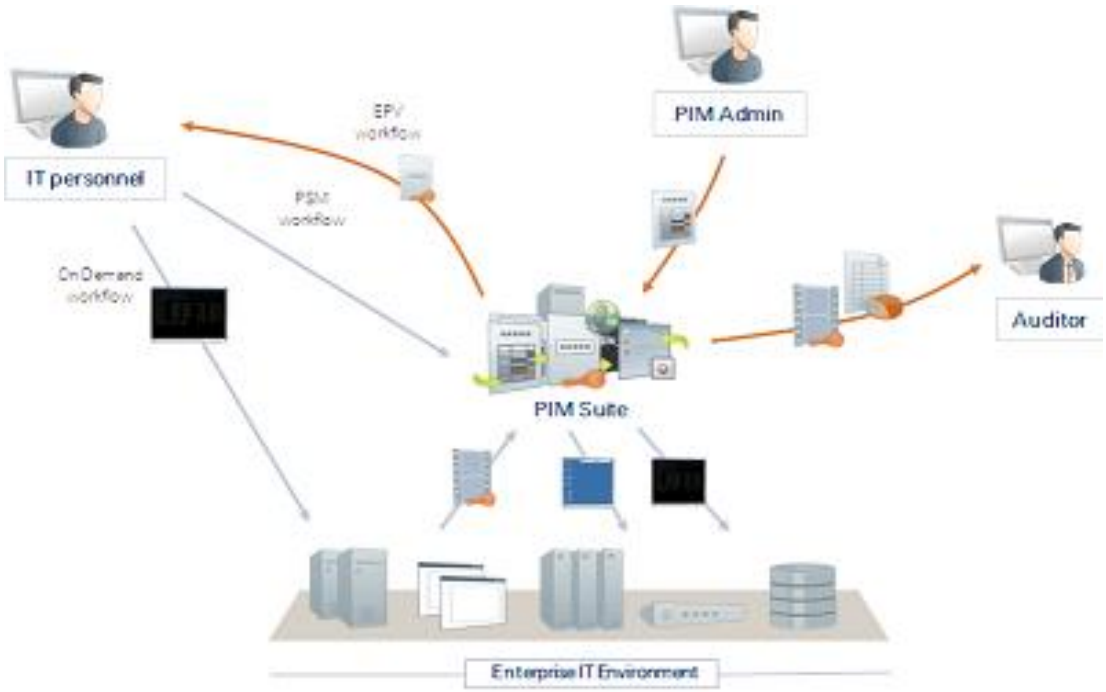


Рис.2.2. Архітектура рішення безпеки привілейованого доступу

Сховище

Цифрове сховище CyberArk є найбезпечнішим місцем у мережі, де можуть зберігатися конфіденційні дані. Vault призначений для встановлення на спеціальному комп'ютері для повної ізоляції даних. Він оснащений найсучаснішою технологією безпеки та вже налаштований і готовий до використання після встановлення. Це означає, що система безпеки не потребує досвіду безпеки або складної конфігурації для роботи на максимальній потужності.

Постійний доступ до паролів є надзвичайно важливим. У разі збою сервера доступ до паролів може бути тимчасово заблоковано. Vault можна встановити як кластер серверів високої доступності, який забезпечує постійний доступ до

облікових записів у Vault. У цій реалізації завжди є один сервер, який перебуває в режимі очікування на випадок збою іншого сервера в кластері.

Vault є повноцінним клієнтом LDAP (Lightweight Directory Access Protocol) і може прозоро спілкуватися з LDAP-сумісними серверами каталогів для отримання ідентифікаційної інформації користувача та інформації про безпеку. Це забезпечує автоматичне надання та створення унікальних та індивідуальних користувачів на основі членства в зовнішній групі та атрибутів.

Сайт аварійного відновлення безпеки з привілейованим доступом забезпечує регулярну реплікацію сховища в сховище аварійного відновлення та може негайно взяти на себе роботу, коли виробниче сховище раптово припиняє обробку запитів.

Сховище встановлено з інтерфейсом, який дозволяє адміністратору запускати та зупиняти Сховище, а також контролювати його роботу.

Інтерфейс веб-доступу Password Vault

Веб -доступ до сховища паролів (PVWA) — це повнофункціональний веб-інтерфейс, який надає єдину консоль для запиту, доступу та керування привілейованими паролями в масштабах підприємства як кінцевими користувачами, так і адміністраторами, які майже не навчаються.

Автоматично створені списки часто використовуваних паролів і нещодавно використаних паролів для кожного користувача полегшують швидкий доступ і використання. Крім того, Mobile PVWA дозволяє користувачам отримувати доступ до привілейованих облікових записів із мобільних пристроїв, забезпечуючи безперебійне підключення та оптимальні робочі процеси.

Простий, інтуїтивно зрозумілий майстер PVWA дозволяє користувачам визначати нові привілейовані паролі, а потужний механізм пошуку дозволяє знаходити привілейовані паролі та конфіденційні файли з мінімальними зусиллями.

Інформаційна панель CyberArk PVWA дає змогу переглянути огляд активності у рішенні безпеки привілейованого доступу, а також статистику всіх дій, які мали місце. Інформаційна панель показує графічне представлення паролів,

якими керували, і посилання на певну інформацію про користувачів і паролі, які потребують особливої уваги.

Адміністративні інтерфейси PrivateArk

Клієнт PrivateArk — це звичайна програма Windows, яка використовується як адміністративний клієнт для рішення Privileged Access Security. Його можна встановити на будь-якій кількості віддалених комп'ютерів і отримати доступ до Vault через будь-яку комбінацію LAN, WAN або Інтернету.

Щоб отримати доступ до сховища, користувач-адміністратор сховища повинен визначити користувача в сховищі. Потім адміністратор мережі Vault повинен визначити IP-адресу або IP-маску комп'ютера, на якому встановлено клієнт PrivateArk, у мережевій зоні Vault.

Крім того, користувач має бути автентифікований Сховищем, перш ніж отримати доступ. Рішення Privileged Access Security забезпечує високозахищену систему автентифікації користувачів за допомогою настроюваної комбінації паролів, фізичних ключів і сертифікатів.

Після автентифікації користувач може працювати з клієнтом PrivateArk, щоб налаштувати ієрархію Сховища та створити сейфи та користувачів. Властивості сейфа визначають спосіб доступу до кожного сейфа, а спеціальні властивості користувача визначають паролі, до яких кожен користувач може отримати доступ, і рівень контролю, який він має над цими паролями. Користувачі також можуть контролювати та відстежувати дії зі своїм паролем, зокрема, хто, коли та звідки отримав доступ до їхньої інформації.

Кожна команда, запит, передача файлів і конфігурація користувача шифруються перед передачею між Vault і клієнтом PrivateArk, щоб забезпечити максимальний захист даних у будь-який час.

Центральний менеджер політики

Рішення Privileged Access Security забезпечує революційний прорив в управлінні паролями за допомогою CyberArk Central Policy Manager (CPM) , який автоматично забезпечує дотримання корпоративної політики. Цей компонент керування паролями може автоматично змінювати паролі на віддалених машинах і

зберігати нові паролі в EPV без втручання людини відповідно до політики організації. Це також дозволяє організаціям перевіряти паролі на віддалених машинах і узгоджувати їх, якщо це необхідно.

CPM генерує нові випадкові паролі та замінює існуючі паролі на віддалених машинах. Потім нові паролі зберігаються в EPV, де вони користуються всіма функціями доступності та безпеки EPV.

Завдяки розподіленій архітектурі рішення Privileged Access Security додаткові CPM можна встановити в різних мережах для керування паролями, які зберігаються в одному сховищі. Vault також підтримує спільні файли конфігурації для додаткових CPM у реалізаціях високої доступності та керування паролями для кожного Safe у реалізаціях із балансуванням навантаження. Ця гнучкість дає змогу рішенню Privileged Access Security підтримувати складні розподілені середовища, наприклад, де кількома центрами обробки даних керує одне сховище.

Привілейований менеджер сеансу

Менеджер привілейованих сеансів (PSM) дозволяє організаціям захищати, контролювати та відстежувати привілейований доступ до мережевих пристроїв. Використовуючи технологію Vaulting, він керує доступом до привілейованих облікових записів у централізованій точці та сприяє точці керування для ініціювання привілейованих сеансів. PSM забезпечує дотримання правил, які визначають, які користувачі мають право на доступ до привілейованих облікових записів, коли та з якою метою. Крім того, PSM контролює, до яких протоколів підключення користувач може отримати доступ, дозволяючи організаціям фільтрувати обмежені протоколи. PSM може записувати всі дії, які відбуваються під час привілейованого сеансу, у компактному форматі та забезпечувати детальний аудит сеансу та відтворення, схоже на DVR. Записи зберігаються та захищаються на сервері Vault і доступні для авторизованих аудиторів.

Підприємства можуть використовувати PSM для забезпечення безпечного віддаленого доступу сторонніх постачальників до конфіденційних мережевих ресурсів без розголошення конфіденційних паролів або ключів і під час запису всього сеансу. Усе це можна зробити за допомогою протоколу HTTPS, без

необхідності відкривати брандмауер підприємства для власних протоколів, таких як SSH і RDP, або за допомогою стандартних клієнтів RDP, які дозволяють користувачеві підключатися безпосередньо зі свого робочого столу до цільової машини.

PSM також може обмежити неавторизовані команди, якщо вони виконуються привілейованим користувачем на мережевому пристрої або будь-якій цільовій системі на основі SSH.

PSM відокремлює кінцевих користувачів від цільових машин і ініціює привілейовані сеанси без розголошення паролів або ключів, зберігаючи найвищий рівень безпеки, характерний для всіх компонентів CyberArk.

Крім того, PSM може відображати широкий огляд усіх дій, що виконуються на кожному привілейованому обліковому записі без винятку. Вся діяльність повністю контролюється та відповідає суворим стандартам аудиту.

PSM інтегрується з CyberArk Privileged Threat Analytics (PTA), щоб організації могли визначати привілейовані сеанси з високим рівнем ризику в реальному часі. Ця здатність виявляти порушення або потенційно зловмисну діяльність значно підвищує безпеку організації, дозволяючи аудиторам зосередитися на перевірці та негайно реагувати.

PSM прозоро та бездоганно інтегрується в існуючу корпоративну інфраструктуру та не потребує змін у робочому процесі користувачів, паролях або процедурах доступу до ключів.

Привілейований менеджер сеансів для SSH

Привілейований менеджер сеансів для SSH (PSM для SSH) дозволяє організаціям захищати, контролювати та відстежувати привілейований доступ до мережевих пристроїв. Використовуючи технологію Vaulting, він керує доступом до привілейованих облікових записів у централізованій точці та сприяє точці керування для ініціювання привілейованих сеансів. PSM для SSH точно визначає користувачів, які мають право використовувати привілейовані облікові записи та ініціювати привілейований сеанс, коли та з якою метою. PSM для SSH може записувати всі дії, які відбуваються в привілейованому сеансі, у компактному

форматі. Текстові записи зберігаються та захищені на сервері Vault і доступні для авторизованих аудиторів. PSM для SSH також надає привілейовані можливості єдиного входу та дозволяє користувачам підключатися до цільових пристроїв без доступу до привілейованого пароля або ключа підключення.

PSM для SSH можна інтегрувати з Microsoft Active Directory (AD) для прозорого забезпечення користувачів у системах UNIX, оптимізуючи керування користувачами та зменшуючи адміністративні витрати. Окрім автоматичного налаштування користувачів, це рішення CyberArk має переваги всіх стандартних функцій безпеки та керування CyberArk, включаючи контроль доступу та аудит. Користувачі мають миттєвий доступ до машин UNIX на основі своїх дозволів і груп AD, що сприяє безперебійному робочому процесу та підтримці продуктивності.

PSM для SSH також може обмежувати неавторизовані команди, якщо вони виконуються привілейованим користувачем на мережевому пристрої або будь-якій цільовій системі на основі SSH.

PSM для SSH відокремлює кінцевих користувачів від цільових машин і ініціює привілейовані сеанси без розголошення паролів або ключів, зберігаючи найвищий рівень безпеки, типовий для всіх компонентів CyberArk. Крім того, PSM для SSH P може відображати широкий огляд усіх дій, що виконуються на кожному привілейованому обліковому записі без винятку. Вся діяльність повністю контролюється та відповідає суворим стандартам аудиту.

PSM для SSH інтегрується з CyberArk Privileged Threat Analytics (PTA), щоб дозволити організаціям визначати привілейовані сеанси з високим ризиком у реальному часі.

Привілейований менеджер сеансів для Інтернету

Адміністратори програмного забезпечення як послуги (SaaS), інфраструктури як послуги (IaaS), платформи як послуги (PaaS) і привілейовані бізнес-користувачі часто мають широкий і необмежений доступ до ряду соціальних мереж , веб-програми та хмарні консолі керування. Ці високопривілейовані користувачі часто є об’єктами кібератак у гібридних і хмарних середовищах.

Privileged Session Manager for Web (PSM for Web), як частина рішення CyberArk Privileged Access Security, надає сучасним корпоративним організаціям власний уніфікований підхід до захисту доступу до багатьох хмарних платформ, програм і служб, який зберігає переваги Privileged Session Manager, наприклад як ізоляція, контроль і моніторинг.

PSM for Web інтегрується з CyberArk Privileged Threat Analytics (PTA), щоб дозволити організаціям визначати привілейовані сеанси з високим рівнем ризику в режимі реального часу. Ця здатність виявляти порушення або потенційно зловмисну діяльність значно підвищує безпеку організації, дозволяючи аудиторам зосередитися на перевірці та негайно реагувати.

PSM для Інтернету прозоро та легко інтегрується в існуючу корпоративну інфраструктуру та не потребує змін у робочому процесі користувачів, паролях чи процедурах доступу до ключів.

Менеджер привілеїв на вимогу

Менеджер привілеїв на вимогу (OPM) CyberArk дозволяє організаціям захищати, контролювати та відстежувати привілейований доступ до команд UNIX за допомогою технології Vaulting, щоб дозволити кінцевим користувачам виконувати завдання суперкористувача за допомогою власного особистого облікового запису, зберігаючи при цьому концепцію найменших привілеїв. Це комплексне рішення, яке розширює можливості IT-спеціалістів і забезпечує повну видимість і контроль суперкористувачів і привілейованих облікових записів у всьому підприємстві. Використовуючи OPM, повне рішення Privileged Access Security забезпечує централізоване керування та аудит від уніфікованого продукту до всіх аспектів керування привілейованим обліковим записом.

Привілейований аналіз загроз

Оскільки привілейовані облікові записи найчастіше зламуються під час атаки, CyberArk Privileged Threat Analytics (PTA) постійно відстежує використання привілейованих облікових записів, які керуються на платформі CyberArk Privileged Access Security (PAS), а також облікових записів, якими ще не керують. CyberArk і шукає ознаки зловживань або неправильного використання платформи CyberArk.

PTA також шукає зловмисників, які компрометують привілейовані облікові записи, запускаючи складні атаки, такі як Golden Ticket.

PTA є частиною рішення CyberArk Privileged Access Security і забезпечує додатковий рівень безпеки, який виявляє зловмисну активність, спричинену привілейованими обліковими записами, і проактивно запобігає поточним атакам. PTA підтримує виявлення зловмисних дій у привілейованих облікових записах за умови автентифікації за допомогою паролів або ключів SSH.

Використовуючи власні алгоритми профілювання, PTA розрізняє в режимі реального часу нормальну та ненормальну поведінку та подає сповіщення, коли виявляється аномальна активність. Таким чином, він використовує можливості CISO для зниження ризику внутрішніх загроз, шкідливих програм, цілеспрямованих атак і APT, які використовують привілейованих користувачів для здійснення атак. Це значно зменшує здатність цих факторів загрози проникати в систему та усуває один із найбільших ризиків для вашої організації.

Використовуючи технологію DPI та підключаючись до мережі організації, PTA може детерміновано виявляти атаки Kerberos і сповіщати про них у режимі реального часу.

PTA також активно відстежує ризики, пов’язані з критично важливими привілейованими обліковими записами в IT-середовищі, якими може зловживати зловмисник. PTA надсилає сповіщення команді безпеки, щоб упоратися з цими ризиками, перш ніж зловмисники ними зловживають.

PTA обробляє мережевий трафік і отримує необроблені події від Vault вашої організації, комп’ютерів UNIX і Windows, а також отримує додаткові вхідні дані за допомогою запитів до Active Directory, потім виявляє події безпеки в режимі реального часу та надсилає їх як сповіщення електронною поштою на власну інформаційну панель PTA. або на інформаційну панель SIEM.

Загалом PTA робить наступне:

– Виявляє аномалії, пов’язані з привілейованими обліковими записами: виявлення аномалій у використанні привілейованих облікових записів, наприклад використання, яке не відбувається протягом звичайних годин використання.

– Виявляє інциденти безпеки , пов’язані з привілейованими обліковими записами: виявляє інциденти безпеки шляхом виконання глибокої перевірки пакетів і пошуку детермінованих характеристик атак Kerberos і додаткових відомих атак, таких як Golden Ticket і зловмисне отримання облікових записів домену (DC Sync).

– Виявляє ризики, пов’язані з привілейованими обліковими записами : виявляє ризики шляхом моніторингу та сповіщення про критичні ризики в привілейованих облікових записах.

– Містить інциденти безпеки: генерує корисну інформацію для підтримки швидкого й автоматичного реагування на інциденти.

Щоб точно визначити ненормальну діяльність привілейованих користувачів, PTA використовує різні статистичні алгоритми. Ці алгоритми генерують профілі системних дій, а наступні дії шукають відхилення від цих профілів. Відхилення, які є підозрілими та становлять потенційний ризик, класифікуються як інциденти безпеки.

Утиліта завантаження пароля

Утиліта Password Upload завантажує кілька об’єктів паролів до рішення Privileged Access Security, роблячи процес впровадження Vault швидшим і більш автоматичним. Ця утиліта працює шляхом масового завантаження паролів та їхніх властивостей у сховище із заздалегідь підготовленого файлу, створюючи необхідне середовище, коли це необхідно. Він запускається з командного рядка щоразу, коли потрібно завантажити пароль.

Інтерфейси SDK

Application Password SDK позбавляє від необхідності зберігати паролі програм, вбудовані в програми, сценарії або файли конфігурації, і дозволяє централізовано зберігати, реєструвати та керувати цими високочутливими паролями в рамках рішення Privileged Access Security. Завдяки цьому унікальному

підходу організації можуть відповідати внутрішнім і нормативним вимогам щодо періодичної заміни пароля та контролювати привілейований доступ до всіх систем, баз даних і програм. Application Password SDK надає різноманітні API, зокрема Java, .Net, COM, CLI та C/C++.

Постачальник паролів програм — це «локальний сервер», який безпечно кешує паролі після того, як їх було отримано зі сховища, і забезпечує миттєвий доступ до паролів, незалежно від продуктивності мережі.

Постачальник облікових даних сервера програм безпечно й автоматично керує обліковими даними сервера програм, які зберігаються в XML-файлах джерела даних. Це запобігає необхідності виконувати будь-які зміни коду додатків і може виконувати заміну пароля без необхідності перезапускати сервер додатків, таким чином усуваючи простої та забезпечуючи безперервність бізнесу.

Адміністративні API

Інтерфейс командного рядка CyberArk Vault (PACLI) дозволяє користувачам отримувати доступ до рішення безпеки привілейованого доступу з будь-якого місця за допомогою автоматичних сценаріїв у надзвичайно інтуїтивно зрозумілому середовищі командного рядка.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

3.1 Технологія управління привілейованим доступом

Менеджер привілейованого доступу – автономна архітектура

Технологія PAM – надає організаціям можливість бути впевненими що всі адміністративні паролі будуть безпечно архівуватися, передаватись і надаватися авторизованим користувачам, таким як IT-персонал, адміністраторам і локальним адміністраторам у віддалених місцях.

Технологія забезпечує кілька рівнів безпеки (включно з брандмауером, VPN, автентифікацією, контролем доступу, шифруванням тощо), які є основою технології PAM – Self-Hosted.

Технологія PAM — Self-Hosted — вимагає мінімальних зусиль для налаштування та може бути повністю функціональною за дуже короткий період часу. На рис.3.1. показано, як компоненти технології PAM – Self-Hosted взаємодіють між собою.

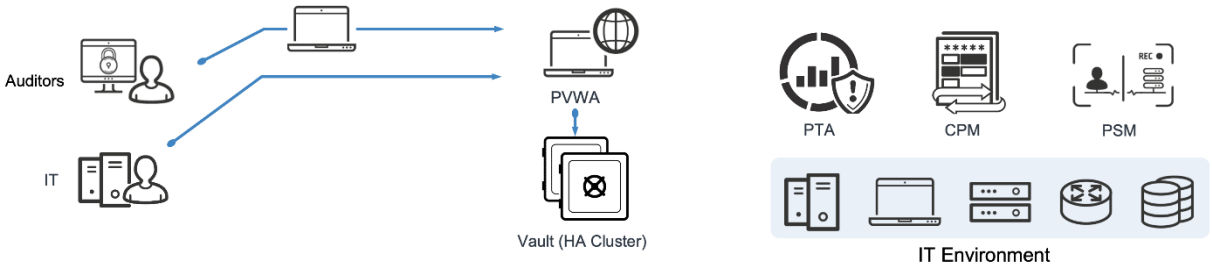


Рис. 3.1. Взаємодія компонентів технології PAM

Технологія рішення PAM – Self-Hosted складається з двох основних елементів. Одним з них є Storage Engine (який також називають «сервером» або просто «сховищем»), який зберігає дані та відповідає за безпеку даних у стані спокою та забезпечення автентифікованого та контрольованого доступу.

Другим елементом є інтерфейс (інтерфейси Windows, веб-інтерфейси та пакети SDK), який взаємодіє з системою зберігання, з одного боку, і надає доступ користувачам і програмам, з іншого. Storage Engine та інтерфейс взаємодіють за допомогою безпечного протоколу CyberArk – протоколу Vault.

Першим етап впровадження технології є єішення Privileged Access Security, яке використовує розподілені сховища для задоволення потреб у доступності в різних регіонах глобальних організацій. Це рішення усуває залежність від одного Vault і забезпечує підвищену продуктивність і відмовостійкість завдяки роботі з локальним Vault. Клієнти можуть переконатися, що доступ до їхніх найважливіших активів доступний, і вони можуть отримати облікові дані свого облікового запису, ініціювати сеанси та продовжувати сеанси незалежно від стану мережі чи основного сховища.

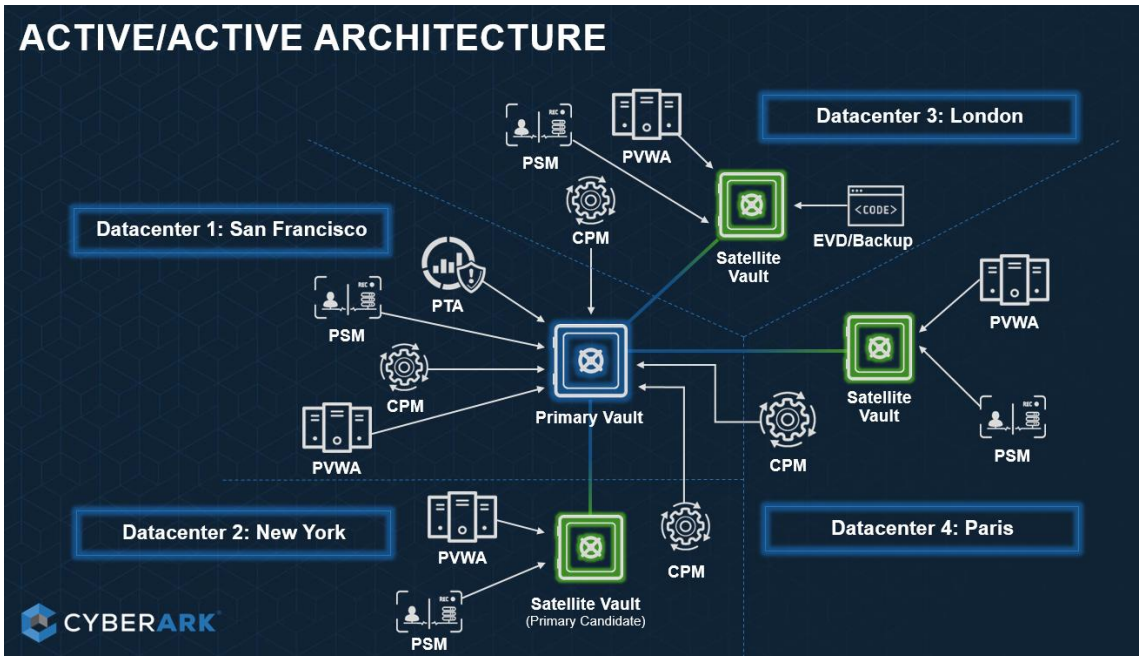


Рис.3.2. Розподілене середовище сховища привілейованих даних [8]

Рішення Distributed Vaults базується на одному основному сховищі та кількох супутникових сховищах:

Основне сховище – основне сховище, яке надає послуги читання та запису та є єдиним джерелом даних, з якого копіюються всі інші сховища [8].

Супутникові сховища – копії сховищ, які надають повні послуги, коли основне сховище доступне, і послуги лише для читання, коли основне сховище недоступне [8].

Кандидат у первинне сховище – одне з супутникових сховищ, яке було попередньо визначено для автоматичного просування як нового основного сховища, якщо первинне сховище не працює.

Усі сховища в середовищі розподілених сховищ повністю синхронізовані. Це досягається шляхом асинхронної реплікації критичної інформації в базі даних, що надсилається Основним сховищем у режимі реального часу та через захищений протокол CyberArk до всіх супутникових сховищ. Файли, які мають відношення до звітів і записів, тиражуються з меншою частотою, яку можна налаштувати.

Компоненти PAS, які є частиною можливості забезпечення постійного доступу до найбільш важливих активів клієнтів – PVWA, PSM і AAM – можна налаштувати для роботи з будь-яким Vault у розподіленому середовищі Vaults, тоді як інші компоненти PAS можуть бути лише налаштовано для роботи з основним сховищем. Компоненти, які можна налаштувати для Satellite Vault, можуть безперебійно працювати, доки існує зв’язок між Satellite Vault і Primary Vault, а також Primary Vault працює. Усі дії, які включають чисті операції читання, надаються незалежно Satellite Vault, тоді як дії, які включають операції запису, направляються Satellite Vault до основного сховища [8].

У разі збою або розриву зв’язку між основним сховищем і супутниковим сховищем супутникове сховище все ще може обслуговувати запити, які базуються на чистих транзакціях читання, але, щоб гарантувати постійне виконання вимог відповідності, супутникове сховище також може зберігати записи аудиту та направляти їх назад до основного сховища через фіксований інтервал часу [8].

Можливості розподілених сховищ CyberArk дозволяють вашим програмам отримати вигоду від високої доступності, надаючи активні послуги для таких функцій:

Отримання облікових даних програми. Дозвольте клієнтським програмам скористатися високою доступністю CyberArk Vault, гарантуючи, що постачальник

облікових даних завжди зможе отримати облікові дані, оскільки завжди є доступне сховище для відповіді на запити облікових даних [8].

Отримання облікових даних користувача – дозвольте користувачам отримувати облікові дані облікового запису в будь-який час незалежно від статусу конкретного сховища.

Керування сеансом – дозвольте користувачам ініціювати та підтримувати привілейований сеанс незалежно від доступності основного сховища або розташування PVWA, з якого було зроблено запит на ініціювання сеансу. Це актуально для підключень, які ініціюються через PSM з файлами RDP, PSM для SSH і PSM з HTML5.

Кожен запит, зроблений від імені цих служб для отримання інформації з цифрового сховища, обслуговується, навіть якщо сховище недоступне, оскільки завжди є інше сховище, яке може відповісти.

Крім того, уся інформація, створена під час збою (аудити, метадані сеансу, записи), зберігається локально та консолідується в основному сховищі після відновлення з’єднання між основним і супутниковим сховищами, що гарантує відсутність втрати даних.

Процес встановлення розподілених сховищ складається з кількох етапів. Кожен із основних етапів має власний майстер інсталяції, який інтуїтивно проведе вас через інсталяцію. Ви повинні інсталювати рішення Distributed Vaults у правильному порядку, щоб кожен компонент міг інсталювати свою повну функціональність.

У таблиці 3.1. описано процедуру встановлення розподілених сховищ.

Крок	Довідка
Перед встановленням: Сховище PVWA PTA	Сплануйте архітектуру свого середовища розподілених сховищ. Вирішіть, де встановити основне сховище та де встановити супутникові сховища.

	Відповідно до кількості супутникових сховищ заплануйте кількість користувачів DR, які копіюватимуть основне сховище до супутникових сховищ. Усі сховища в середовищі розподілених сховищ мають бути синхронізовані з NTP-сервером організації, щоб гарантувати, що діяльність сховища синхронізована із записами на всіх інших серверах.
Встановіть основне сховище	Встановіть CyberArk Primary Vault: Встановіть програму Vault. Встановіть програму Disaster Recovery. Налаштуйте сховище як основне.
Встановіть Satellite Vault	Встановіть CyberArk Satellite Vault: Встановіть програму Satellite Vault. Встановіть програму Disaster Recovery. Налаштуйте Vault як супутник. Після завершення встановлення всіх супутникових сховищ: Перезапустіть службу аварійного відновлення CyberArk. Vault на кожному з супутникових сховищ.
Встановіть компоненти PVWA PSM PSM для SSH інші компоненти	Встановіть компоненти розподілених сховищ.
Встановіть резервну копію та EVD	Встановіть утиліти резервного копіювання та експорту даних сховища для розподілених сховищ.
Після встановлення	Після встановлення. Після встановлення - Компоненти.

Сховище PVWA PTA	Налаштуйте керування ключами HSM у середовищі .розподілених сховищ.

Другим етапом впровадження технології є налаштування постачальника облікових даних CyberArk Secrets Manager, частина рішення Privileged Access Security, використовується для видалення жорстко закодованих облікових даних програми, вбудованих у програми, сценарії або файли конфігурації, і дозволяє централізовано зберігати, реєструвати та керувати цими високочутливими паролями в Сховищі. Цей унікальний підхід дозволяє організаціям відповідати внутрішнім і нормативним вимогам щодо періодичної заміни пароля та контролювати привілейований доступ до всіх систем, баз даних і програм [9].

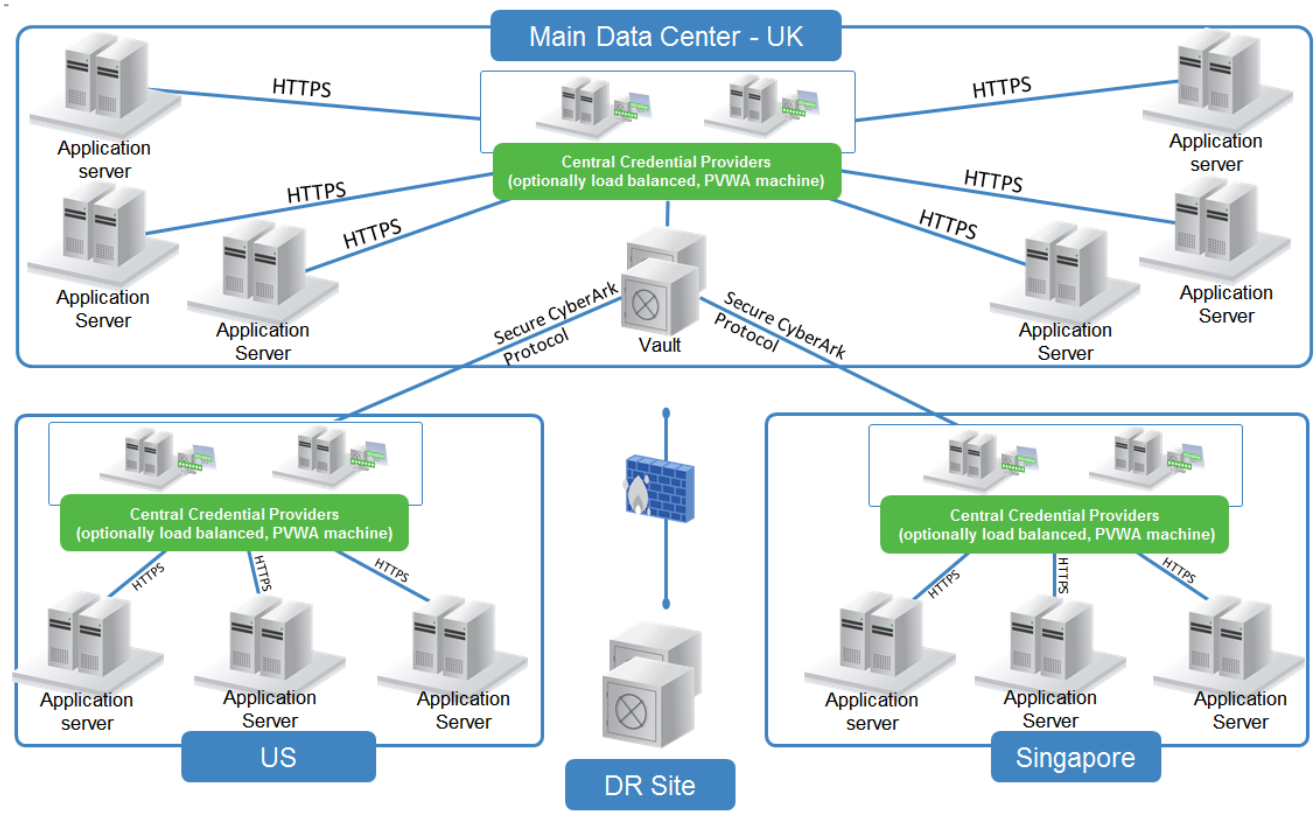


Рис. 3.3. Постачальник облікових даних CyberArk Secrets Manager

Існує три варіанти постачальників облікових даних CyberArk, два з яких є варіантами основного постачальника. Постачальник облікових даних — це служба диспетчера секретів на основі агента, яка дозволяє додаткам на основі ОС

отримувати свої керовані секрети на вимогу. Центральний постачальник облікових даних — це той самий агент, який описано вище, але з додатковим рівнем веб-сервісу, що дозволяє виконувати пошук облікових даних програми віддалено за допомогою команди REST API, а не локально на сервері агента. Постачальник облікових даних сервера додатків (ASCP) — це інший варіант постачальника облікових даних, розроблений для роботи з середовищами виконання Java EE (наприклад, WebSphere, WebLogic, JBoss, Tomcat), і робить це за допомогою рівня абстракції для взаємодії з програмою Java.

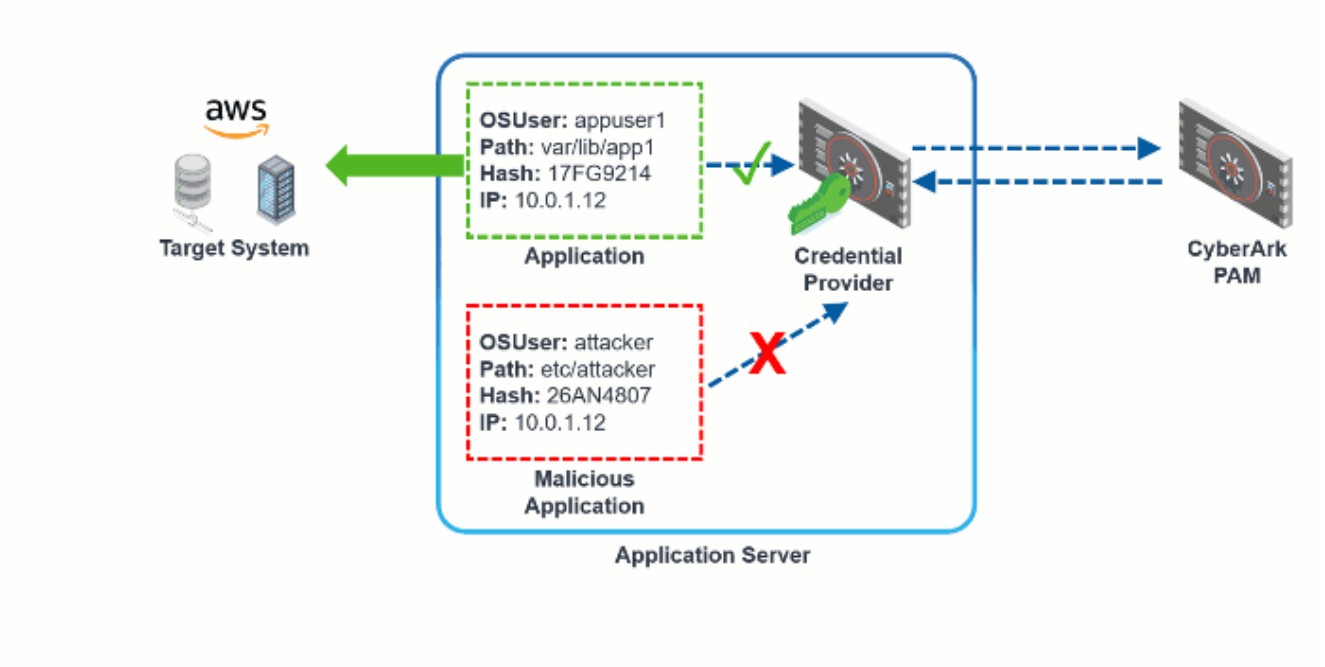


Рис. 3.4. Приклад роботи постачальника облікових записів

Робоче навантаження з будь-яким із варіантів постачальника облікових даних називається «ідентифікатором програми» та визначається в CyberArk PAM (Privilege Cloud або Self-Hosted). Секрети, пов’язані з певним робочим навантаженням, зазвичай зберігаються в одному сейфі в CyberArk PAM. Традиційно існує відповідність 1:1 між робочим навантаженням і безпечним. Сейф можна вважати представленням робочого навантаження в CyberArk PAM. Постачальники облікових даних також повинні надавати доступ до тих самих сейфів, що й робоче навантаження, щоб обслуговувати запитаний секрет. Постачальник і ідентифікатор програми працюють у тандемі, щоб надавати секрети

на вимогу. Під час використання основного постачальника облікових даних (варіанти без CCP або ASCP) зазвичай також існує співвідношення 1:1 між постачальником облікових даних і робочим навантаженням. Це не так у двох інших варіантах, оскільки в цьому випадку Постачальник розподіляється між кількома робочими навантаженнями.

Постачальники облікових даних отримують доступ до сейфів та їхніх облікових записів від імені ідентифікаторів програм. Ідентифікатор програми, і ідентифікатор постачальника облікових даних мають бути членами сейфа, щоб програма могла отримувати секрети із сейфа. Кожному постачальнику облікових даних надаються дозволи лише на читання для всіх секретів цього сейфа.

Для випадків використання, описаних вище, CyberArk PAM по суті полегшує роль постачальника ідентифікаційної інформації для робочого навантаження через ідентифікатор програми. Це те, що надає нелюдському робочому навантаженню цифрову ідентифікацію, яку можна перевірити та використовувати, проти постачальника облікових даних. Ідентифікатори додатків – це те, як ідентифікатор визначається для робочого навантаження та є зв’язком 1:1, що фактично означає, що в PAM ідентифікатор додатка є представленням ідентифікатора робочого навантаження. Це також означає, що ідентифікатор програми та Safe є формами представлення робочого навантаження.

Третій крок, який використовує технологія CyberArk PAM CyberArk PAM Privileged Session Manager (PSM) дозволяє організаціям захищати, контролювати та відстежувати привілейований доступ до мережевих пристроїв за допомогою технології Vaulting для керування привілейованими обліковими записами та створення детальних перевірок сеансів і відеозаписів усіх привілейованих сеансів IT-адміністратора на віддалених машинах (рис.3.5).

PSM дозволяє користувачам входити на віддалені (цільові) машини або безпечно відкривати програми через проксі-машину. Встановлені сеанси в цільових системах повністю ізольовані, а облікові дані привілейованого облікового запису ніколи не відкриваються кінцевим користувачам або їхнім клієнтським програмам і пристроям. Архітектура PSM забезпечує безпеку конфіденційних

привілейованих сеансів, одночасно сприяючи спрощеним і власним робочим процесам для IT-адміністраторів [9].

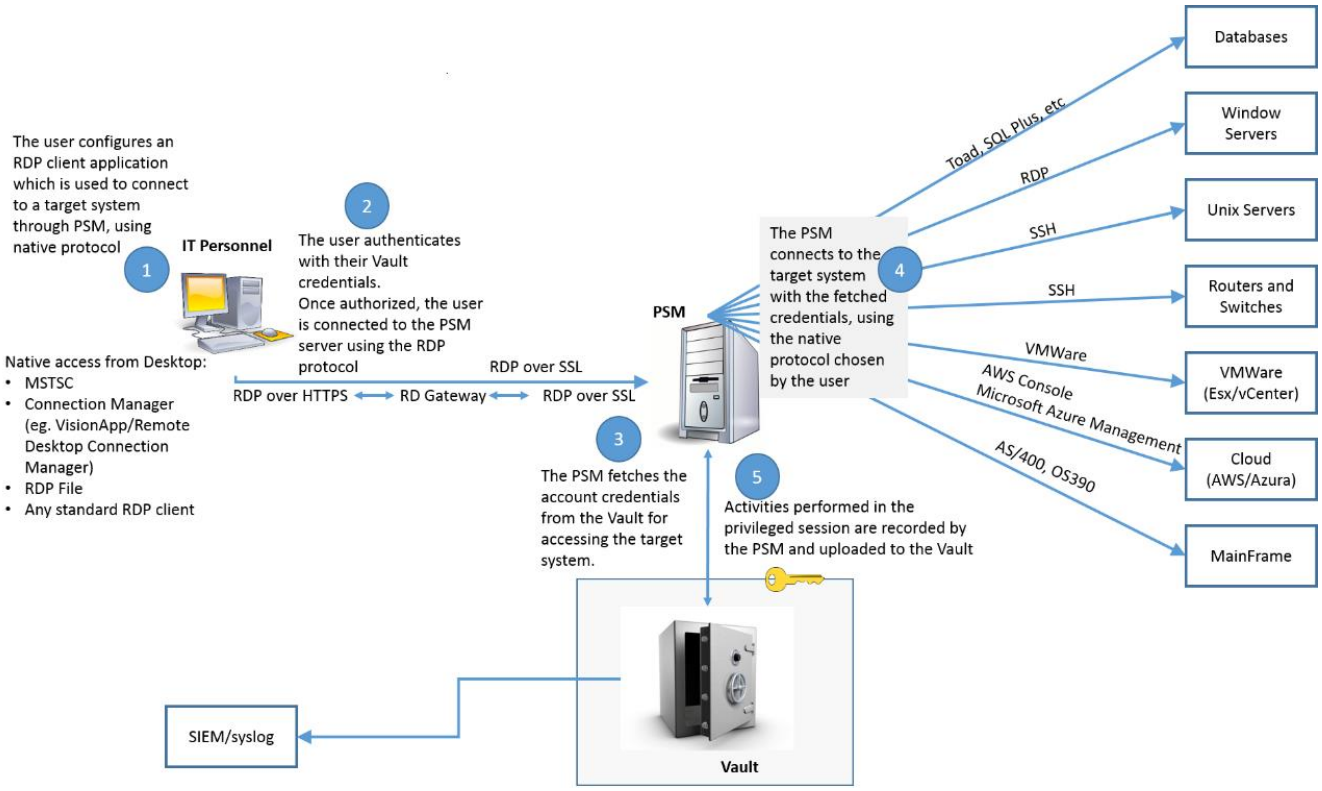


Рис.3.5. Privileged Session Manager

Користувачі можуть підключатися через портал PVWA або альтернативно через PSM для Windows , тобто безпосередньо зі своїх робочих столів за допомогою будь-якої стандартної клієнтської програми RDP, такої як MSTSC, різні диспетчери підключень або файл RDP.

За замовчуванням користувач підключається до машини PSM через порт 3389, використовуючи протокол RDP. Це потрібно для полегшення віддаленого доступу, хоча цей порт зазвичай не відкривається в корпоративному брандмауері, а в деяких випадках це заборонено.

Ви можете налаштувати PSM для забезпечення безпечного віддаленого доступу до цільової машини через шлюз HTML5 під час підключення до порталу PVWA. Шлюз HTML5 тунелює сеанс між кінцевим користувачем і машиною PSM за допомогою безпечного протоколу WebSocket (порт 443). Це усуває вимоги відкривати з’єднання RDP з комп’ютера кінцевого користувача. Натомість

кінцевому користувачеві потрібен лише веб-браузер, щоб встановити з'єднання з віддаленою машиною через PSM.

Крім того, PSM можна налаштувати для роботи зі шлюзом віддаленого робочого стола Microsoft (RDGateway), який тунелює сеанс RDP між користувачем і машиною PSM за допомогою протоколу HTTPS (порт 443). Це забезпечує безпечне з'єднання без необхідності відкривати брандмауер. Уся інформація, яка передається між користувачем і машиною PSM , зашифрована та захищена протоколом HTTPS, який забезпечує безпечний міжмережевий і віддалений доступ.

3.2. Рекомендації використання інформаційної панелі CyberArk PAM

Інформаційна панель надає огляд загального стану системи за вибраний період часу, а також відомості про поточні та минулі інциденти та підсумок активності системи за певний час.

Інформаційна панель, яку показано на рис 3.6, представляє всю інформацію в множинному графічному аналізі активності системи та інцидентів безпеки, що дає змогу побачити та зрозуміти системну діяльність з першого погляду [10].

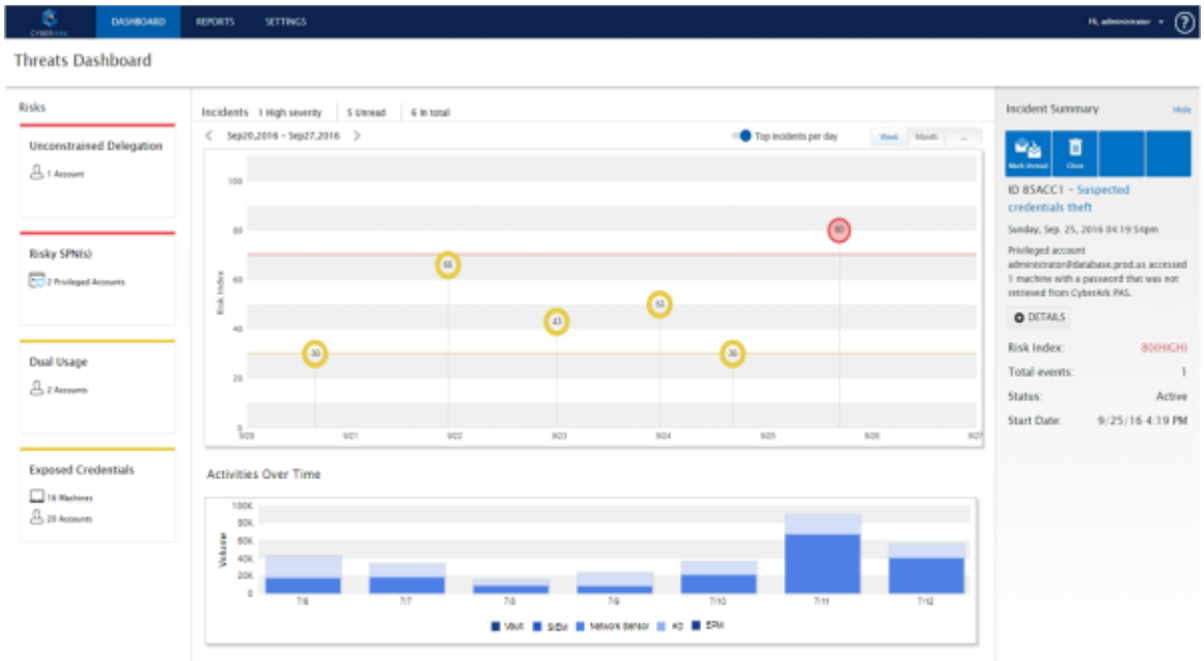


Рис. 3.6. Інформаційна панель

У верхній правій частині інформаційної панелі можна вибрати часовий проміжок для відображення в аналізі інформаційної панелі (Рис.3.6).

Діаграма інцидентів відображає інциденти в системі за вибраний проміжок часу та показує їх серйозність за допомогою таких функцій відображення:

Колір: інциденти відображаються у вигляді кольорових бульбашок відповідно до одного з трьох рівнів ризику. Це дозволяє легко зрозуміти, чи відбувалися підозрілі дії.

Підозрілі дії, виявлені під час привілейованого сеансу, відображаються у великій бульбашці, центр якої також забарвлюється (рис.3.7). Для всіх підозрілих дій, виявлених за вибраний проміжок часу, відображається лише одна підказка. Ця підказка є сукупністю всіх підозрілих дій і розміщується між найбільш підозрілими та останніми підозрілими діями в привілейованому сеансі.

Підозрілі дії, виявлені в привілейованому сеансі, включають:

Команди, які вважаються підозрілими.

Привілейований доступ до Сховища (Vault) в ненормований час.

Надмірний доступ до привілейованих облікових записів у Сховищі.

Активність неактивних користувачів Vault.

Оцінка серйозності: кожна бульбашка містить оцінку, яка вказує на серйозність інциденту. Незважаючи на те, що бульбашки розташовані на різних рівнях діаграми, ця оцінка точно вказує на серйозність.

Рамка: рамка навколо кожної бульбашки вказує на статус керування інцидентом.

Щільний контур вказує на те, що інцидент ще не розглянули.

Світлий контур означає , що інцидент переглянули.

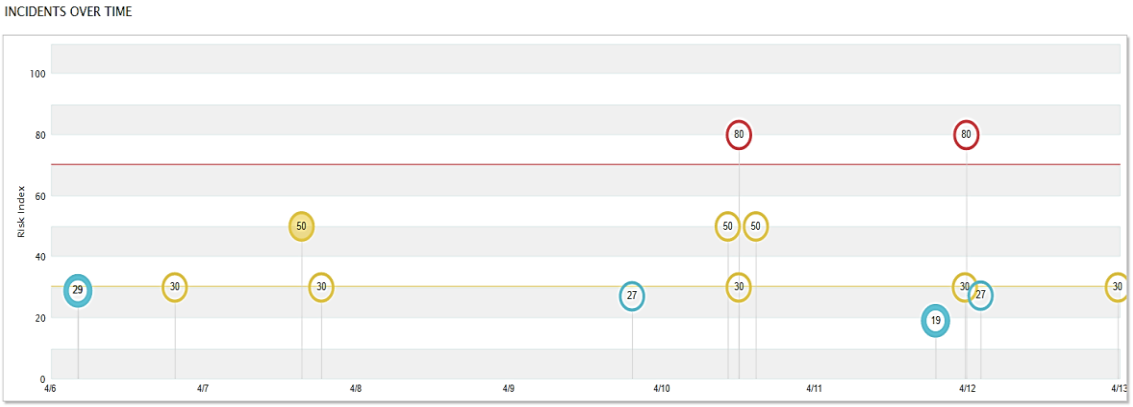


Рис.3.7. Інциденти в системі за вибраний проміжок часу

Для зручності є можливість збільшити відображення періоду часу на діаграмі, щоб чіткіше розрізнити інциденти, які сталися близько один до одного (Рис.3.7).

Клацніть і утримуйте курсор миші на даті, а потім перетягніть її, щоб створити жовте поле, яке визначає відповідний період часу. Ви можете ще більше збільшити вибраний період, повторивши цю процедуру.

Щоб повернутися до типового перегляду діаграми інцидентів, виберіть «Тиждень» у верхній правій частині інформаційної панелі.

Інформаційна панель надає можливість переглянути підсумок подій у системі за вибраний період часу, що дасть змогу порівняти різні типи діяльності. Ця інформація відображається на гістограмі, яка вказує на кількість дій за типом і дату їх виконання (рис.3.8) .

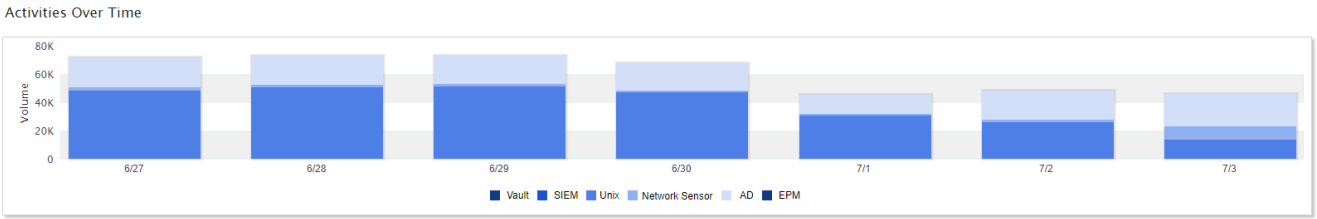


Рис. 3.8. Перегляд підсумок подій

Щоб переглянути підсумок цих дій за певний день, необхідно навести вказівник миші на будь-яку панель. Ви можете натиснути будь-який із типів діяльності внизу. Якщо тип дії сірий, його події не відображаються.

Типи активності отримані від Vault, SIEM, Unix, Network Sensor, AD і EPM. Якщо протягом вибраного періоду часу з одного з цих джерел немає активності, тип не відображається. Дії за період часу до встановлення цієї версії відображаються як тип Усі.

В області подробиць відображається поточний індекс ризику та статус інциденту (рис.3.9).

Зведення про інцидент вказує, чи було врегульовано інцидент, використовуючи такі етапи:

Непрочитаний: цей інцидент ще не переглядався.

На графіку інцидентів цей тип інциденту позначено жирною рамкою .

Активний: цей інцидент розглянуто та наразі розглядається. На графіку «Інциденти» цей тип інцидентів позначено світлою рамкою .

Зачинено: Цей інцидент більше не триває. На графіку інцидентів цей тип інциденту позначено сірою рамкою .

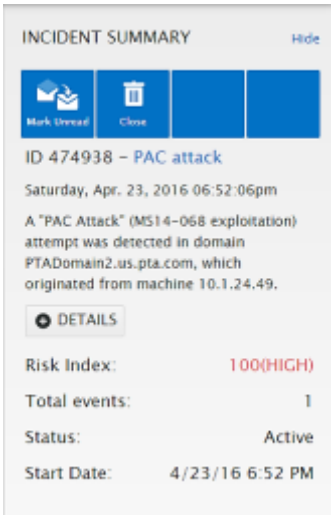


Рис. 3.9. Інформація про інцидент

3.3. Рекомендації щодо створення звітів CyberArk PAM

CyberArk PAM пропонує створення звітів на своїй інформаційній панелі. Для цього необхідно виконати наступні дії:

1. Натиснути «Звіти» , щоб відкрити сторінку «Звіти».

2. Визначте звіт для створення та його вміст:

Діапазон дат – виберіть проміжок часу для включення у звіт. Виберіть одне з наступного:

Останні 7 днів

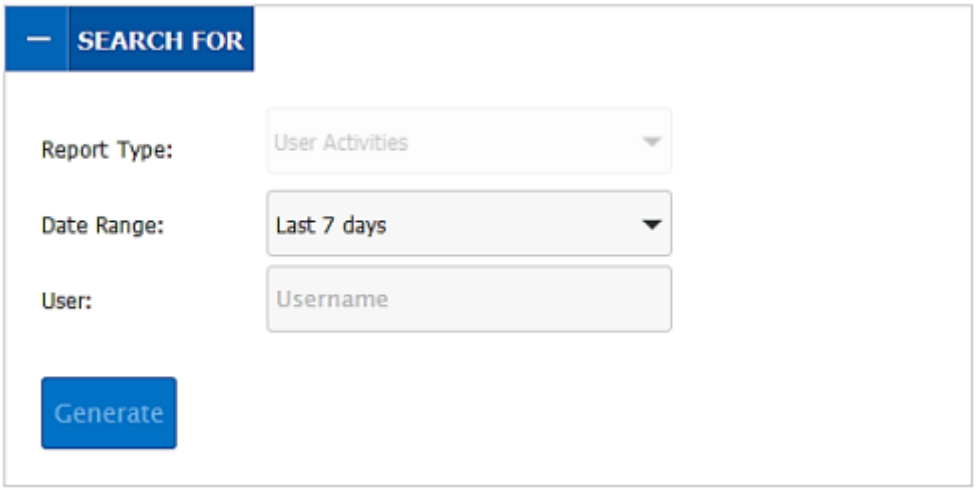
Останні 30 днів

Останні 60 днів

Налаштувати –цей параметр дозволяє відобразити вікно «Вибір діапазону дат», у якому можна вибрати діапазон дат.

Користувач – укажіть ім’я користувача Vault. PTA надає пропозиції під час введення в поле.

На рис.3.10 показано визначення для звіту про дії користувача.



3.10. Налаштування звіту про дії користувача

3. Натисніть Створити , щоб створити звіт за вибраний період часу.

Звіт про дії користувача відображає звичайну поведінку користувача за типом аномалії та відображає всі події, що відбулися за вказаний проміжок часу (рис.3.11).

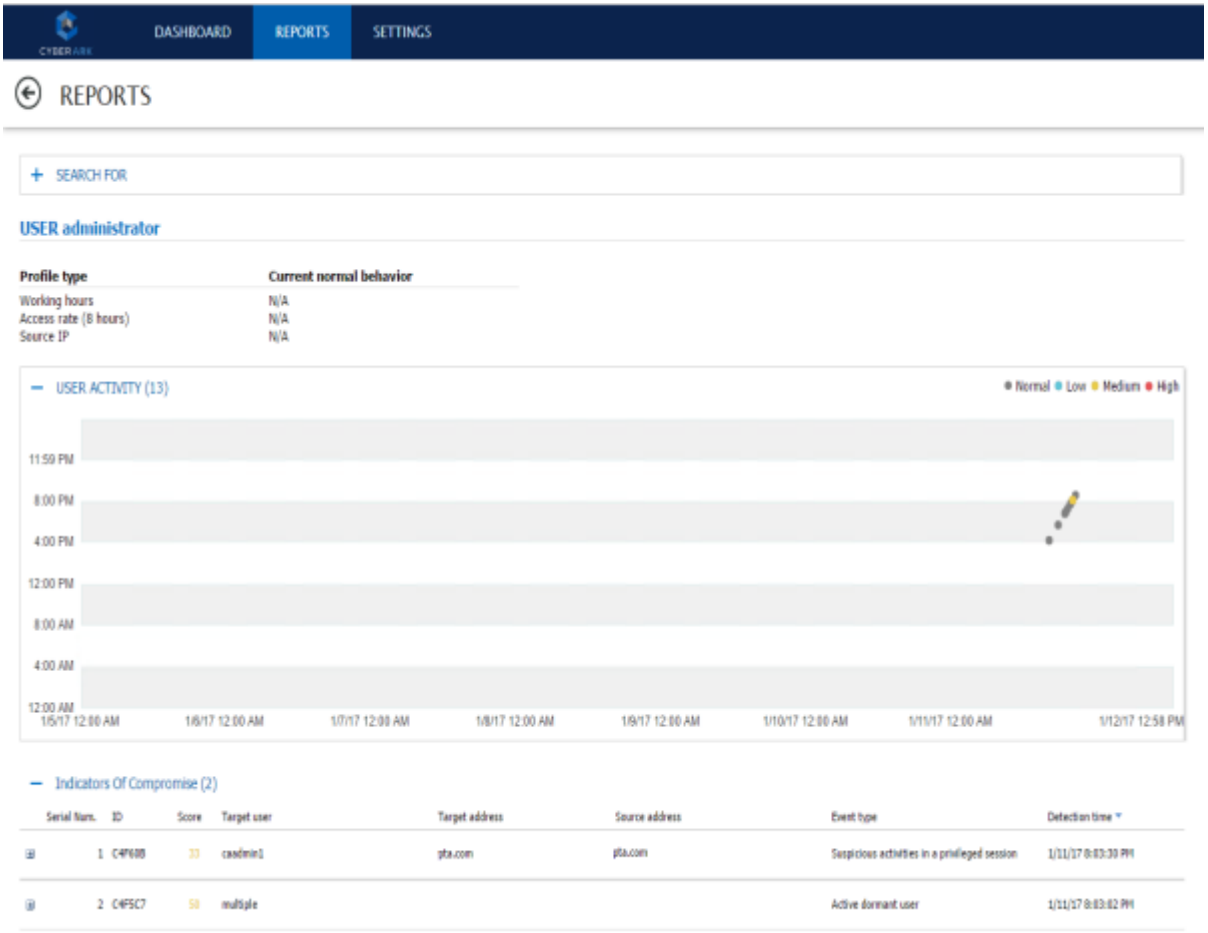


Рис.3.12. Звіт про дії користувача

Звіт про дії користувачів містить такі розділи (рис.3.12):

Підсумок профілю – відображає звичайну поведінку користувача за типом профілю:

Робочий час.

Час доступу (8 годин).

Джерело IP.

Таблиця подій – відображає всі події, які відбулися для цього користувача за вказаний період часу. Таблиця містить такі поля:

Серійний номер – серійний номер аномалії в таблиці.

ID – ідентифікатор аномалії в базі даних PTA .

Оцінка – індекс ризику події.

Цільовий користувач – цільовий користувач, якого вплинула подія.

Цільова адреса – цільова адреса машини, на яку впливає подія.

Адреса джерела – адреса джерела машини, на якій сталася подія.

Тип події – тип події, що сталася.

Час виявлення – час виявлення події.

Звіти в CyberArk PAM можна генерувати за розкладом: щомісяця, щотижня, у визначений час.

Отже запропонована технологія управління привілейованим доступом до інформаційної системи організації CyberArk PAM, надає можливість фахівцям управляти привілейованими користувачами та вчасно реагувати на інциденти кібербезпеки.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проведено аналіз поняття привілейованого доступу та виявлено проблему, яка вказує на необхідності впровадження технології управління привілейованого доступу, що пов’язано з великою кількістю атак на привілейованих користувачів для отримання несанкціонованого доступу до інформаційної системи організації.

В роботі проведено аналіз технологій управління привілейованим доступом на основі використання даних досліджень Gartner. В результаті було обрано для подальшого дослідження технологію від поставщика рішень кібербезпеки CyberArk PAM.

На основі обраного рішення запропоновано архітектуру платформи CyberArk PAM. Компоненти інфраструктури забезпечують масштабованість, надійність та повний захист привілейованого доступу. Гнучка архітектура може починатися з малих розгортань і масштабувати до найбільших та ресурсомістких корпоративних розмірів.

До основних компонентів Endpoint privilege manager, Application access manager, Core Privileged access security надано повний функціональний опис, які поєднуються в єдину технологію управління привілейованим доступом.

В результаті виконання кваліфікаційної роботи отримано технологію управління привілейованим доступом, яка враховує потреби організації та вимагає мінімальних зусиль для налаштування. Така технологія на відміну від інших може бути повністю функціональною за дуже короткий період часу.

Розроблено рекомендації щодо використання інформаційної панелі CyberArk PAM для огляду загального стану системи та створення необхідних звітів для фахівців кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1 10 What is Privileged Access Management. URL: https://www.cyberark.com/what-is/privileged-access-management/ (дата звернення: 12.10.2024).

2. Privileged Access Management. https://www.microsoft.com/ru-ru/security/business/security-101/what-is-privileged-access-management-pam#how-to-implement-pam (дата звернення: 12.10.2024).

3. https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained (дата звернення: 20.10.2024).

4. The Zero Trust Framework and Privileged Access Management (PAM) - Google Books. URL: https://www.google.com.ua/books/edition/The_Zero_Trust_Framework_and_Privileged/MEzyEAAAQBAJ?hl=ru&gbpv=0 (дата звернення: 25.10.2024).

5. Inc. (2024, October 23). Privileged Access Management. URL: https://www.gartner.com/reviews/market/privileged-access-management (дата звернення: 25.10.2024).

6. Harris, C. (2024). Discover the top privileged access management solutions. Explore features such as password management, role-based security, real-time notifications, and reporting. Expert Insights. Retrieved from https://expertinsights.com/insights/the-top-privileged-access-management-pam-solutions (дата звернення: 01.11.2024). .

7. Архітектура рішення безпеки привілейованого доступу | Документи CyberArk. URL: https://docs.cyberark.com/pam-self-hosted/11.3/en/content/pasimp/privileged-account-security-solution-architecture.htm (дата звернення: 15.11.2024).

8. Вступ | Документи CyberArk. (2024, February 13). URL: https://docs.cyberark.com/pam-self-hosted/11.6/en/content/pas%20inst/distributed-vaults-introduction.htm (дата звернення: 16.11.2024).

9. Привілейований менеджер сеансу | CyberArk Docs. (2024, October 03). URL: https://docs.cyberark.com/pam-self-hosted/13.0/en/content/pasimp/privileged-session%20manager-introduction.htm?TocPath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C_____0 (дата звернення: 25.11.2024).

10. Використовуйте та розумійте інформаційну панель | Документи CyberArk. (2024, October 03). URL: https://docs.cyberark.com/pam-self-hosted/13.0/en/content/pta/using-understanding-dashboard.htm?TocPath=End%20user%7CSecurity%20Events%7CClassic%20Interface%7CUse%20and%20Understand%20the%20Dashboard%7C_____0 . (дата звернення: 15.11.2024).

11. Звіти в PVWA. (2024, October 03). Retrieved from https://docs.cyberark.com/pam-self-hosted/13.0/en/content/pasimp/reportsinpvwa.htm?tocpath=End%20user%7CReports%20and%20Audits%7C_____1 (дата звернення: 28.11.2024).

12. Створення звітів | Документи CyberArk. (2024, October 03). Retrieved from https://docs.cyberark.com/pam-self-hosted/13.0/en/content/pta/generating-reports.htm?tocpath=End%20user%7CSecurity%20Events%7CClassic%20Interface%7CGenerate%20Reports%7C_____0 (дата звернення: 02.12.2024).

13. Юхимович А.В., Воротняк М.О., Селітрарь О.О. Підходи до управління привілейованим доступом інформаційної системи організації. *Актуальні проблеми кібербезпеки:* Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Київ, 2024. С. 213-215.