ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

Технологія управління привілейованими користувачами корпоративної інформаційної системи базі рішення Cyberark

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Неділько А. В.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

ЗМІСТ

Стор.

ПЕРЕЛІК СКОРОЧЕНЬ 4

ВСТУП 5

1 АНАЛІЗ ВИМОГ ДО КОРИСТУВАЧІВ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ 7

1.2. Аналіз функцій та призначення корпоративної інформаційної системи 7

1.2. Визначення функцій користувачів корпоративної інформаційної системикористувачі ІС 12

1.3. Аналіз методів та засобів управління привілейованими користувачами 14

2 МЕТОДИ ТА ЗАСОБИ РЕАЛІЗАЦІ СИСТЕМИ УПРАВЛІННЯ ПРВІЛЕЙОВАНИХ КОРИСТУВАЧІВ НА БАЗІ CYBERARK 23

2.1. Життевий цикл системи управління привілейованих користувачів 23

2.2. Обгрунтування принципыв рішення Privileged Access Security 28

2.3. Склад модулів CyberArk Privileged Account Security 34

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІї УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ РІШЕННЯ CYBERARK PRIVILEGED ACCOUNT SECURITY 40

3.1. Рекомендації щодо застосування основних функціональних можливостей Core Privileged Account Security 40

3.2. Рекомендації щодо захист привілейованих облікових записів за допомогою Enterprise Password Vault 43

3.3. Рекомендації використання контролю привілейованого доступу за допомогою Privileged Session Manager 45

3.4. Рекомендації використання Privileged Threat Analytic для визначення і припинення атак в реальному часі 48

ВИСНОВКИ **53**

ПЕРЛІК ПОСИЛАНЬ **54**

ДЕМОНСТРАЦІЙН МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ) **55**

ПЕРЕЛІК СКОРОЧЕНЬ

КІС - Корпоративна інформаційна система

ІС – інформаційна система

БД – база даних

PAM - контроль привілегованих користувачів

SRM - безпеки та управління ризиками

PASM - привілейований аккаунт і управління сесіями

PEDM - управління підвищенням привілеїв і делегуванням

ВСТУП

Актуальність дослідження. Контроль привілейованих користувачів (Privileged Account Management, PAM) - це комплекс рішень, який допомагає здійснювати моніторинг і контроль облікових записів, а також аудит виконуваних дій.

Основною метою таких методів та засобів є запобігання витоків конфіденційної інформації, недопущення збоїв у функціонуванні інформаційних систем, ініційованих діями користувачів привілейованих акаунтів.

Аккаунт з більш широкими можливостями і правами доступу, може стати джерелом витоку даних або піддатися атаці зловмисників. До того ж не виключена його компрометація самим власником.

До основного принципу контролю привілейованих користувачів відносяться керівництво компанії, співробітники, що забезпечують роботу IT-інфраструктури, особи, які здійснюють контроль і аудит.

Для правильної організації контролю привілейованих користувачів потрібно вибирати рішення, які забезпечують моніторинг дій таких акаунтів. Рішення повинно не просто відстежувати активність користувача, але і давати чітку інформацію про те, хто працював під обліковим записом в конкретний момент часу.

Управління доступом до привілейованих облікових записів повинні зберігатися в окремій, від даних звичайних співробітників, зоні.

Тому тема магістерської роботи, щодо впровадження системи привілейованих користувачів є актуальною.

Об'єкт дослідження – процес управління доступом привілейованих користувачів корпоративної інформаційної системи.

Предмет дослідження – технологія управління доступом привілейованих користувачів на базі рішення CyberArk Privileged Access Security.

Мета роботи – розробити рекомендації щодо застосування технології управління доступом привілейованих користувачів на базі рішення CyberArk Privileged Access Security.

Наукові завдання:

проаналізувати основні функції корпоративної інформаційної системи;

проаналізувати види користувачів корпоративної інформаційної системи;

визначити основні компоненти PAM системи та їх функції;

проаналізувати існуючі методи та засоби управління привілейованими користувачами;

розробити рекомендації щодо застосування технології управління привілейованими користувачами на основі рішення CyberArk Privileged Access Security для фахівців з кібербезпеки для управління привілейованими користувачами в корпоративній інформаційній системі.

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

Практичне значення одержаних результатів: рекомендації щодо застосування системи управління привілейованими користувачами в корпоративній інформаційній системі.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ВИМОГ ДО КОРИСТУВАЧІВ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.2. Аналіз функцій та призначення корпоративної інформаційної системи

Корпоративна інформаційна система (КІС) є як сукупність інформаційних ресурсів, процесів і технологій, які збирають, перетворюють і передають корпоративну інформацію. Узагальнена мета корпоративної ІС є накопичення, зберігання і перетворення інформації для використання її в процесі прийняття управлінських рішень для виконання поставлених бізнес-процесів компанії [1].

Сучасні КІС мають складну, часто гетерогенну структуру і призначені для вирішення великої кількості різнотипних завдань автоматизації, що виникають на підприємстві.

Структура і функції КІС, як правило, визначається необхідними завданнями організації і споживачів інформації ІС, серед яких можуть бути як користувачі, так і інші ІС.

Основними завданнями корпоративної ІС є підтримка динамічної інформаційної моделі предметної області і забезпечення вирішення на основі інформаційної моделі задач управлінського, дослідницького, конструкторського, або іншого характеру.

У сучасному світі існує досить велика кількість різновидів інформаційних систем. Класифікація інформаційних систем зазвичай здійснюється на основі будь-яких виділених ознак. Наприклад, з точки зору управлінського рівня, на якому здійснюється використання ІС, прийнято ділити корпоративні ІС на наступні види:

- ІС для забезпечення поточних бізнес-операцій.
- ІС для підтримки процесу прийняття рішень.
- ІС для забезпечення стратегічних переваг.

Як правило КІС повинна підтримувати велику кількість програмних продуктів та різноманітних сервісів. КІС об’єднує в собі ERP, CRM, MRP та інші системи.

Рис 1.1. Архітектура корпоративної інформаційної системи

Перейдемо до області застосування інформаційних систем. Сьогодні комп'ютер став невід'ємною частиною управлінської системи підприємств. Однак сучасний підхід до управління передбачає ще й вкладення грошей в нові інформаційні технології. Причому чим більше підприємство, тим більше повинні бути подібні вкладення [8].

Завдяки стрімкому розвитку інформаційних технологій відбувається розширення області застосування КІС. Якщо раніше мало не єдиною областю, у якої застосовувалися інформаційні системи, була автоматизація бухгалтерського обліку, то зараз спостерігається впровадження інформаційних технологій в багато інших галузях. Ефективне використання корпоративних інформаційних систем дозволяє робити більш точні прогнози і уникати можливих помилок в управлінні.

З будь-яких даних і звітів про роботу підприємства можна витягти масу корисних відомостей. Інформаційні системи якраз і дозволяють отримувати максимум користі з усієї наявної в компанії інформації.

Саме цим фактом і пояснюються життєздатність і бурхливий розвиток інформаційних технологій - сучасний бізнес вкрай чутливий до помилок в управлінні, і для прийняття грамотного управлінського рішення в умовах невизначеності і ризику необхідно постійно тримати під контролем різні аспекти фінансово-господарської діяльності підприємства (незалежно від профілю його діяльності). Тому можна цілком обгрунтовано стверджувати, що в жорсткій конкурентній боротьбі великі шанси на перемогу має підприємство, яке використовує в управлінні сучасні інформаційні технології.

Розглянемо найбільш важливі завдання, які вирішуються за допомогою спеціальних програмних засобів [1].

Бухгалтерський облік. Це класична область застосування інформаційних технологій і найбільш часто реалізується в КІС. Такий стан можна пояснити. По-перше, помилка бухгалтера може коштувати дуже дорого, тому очевидна вигода використання можливостей автоматизації бухгалтерії. По-друге, завдання бухгалтерського обліку досить легко формалізується, так що розробка систем автоматизації бухгалтерського обліку не представляє технічно складної проблеми. Але вимагає постійної підтримки з боку програмістів та відділу безпеки.

Управління фінансовими потоками. Впровадження інформаційних технологій в управління фінансовими потоками також обумовлено критичністю цією галузю

управління підприємства до помилок. Помилка при побудові системи розрахунків з постачальниками і споживачами, може викликати кризу готівки навіть при налагодженій мережі закупівлі, збуту і хорошому маркетингу. І навпаки, правильно розроблені контрольовані умови фінансових розрахунків можуть істотно збільшити дохід компанії.

Управління складом, асортиментом, закупівлями. Далі, можна автоматизувати процес аналізу руху товару, тим самим, відстеживши і зафіксувавши ті двадцять відсотків асортименту, які приносять вісімдесят відсотків прибутку.

Управління виробничим процесом. Управління виробничим процесом є дуже трудомістке завдання. Основними механізмами тут є планування і оптимальне управління виробничим процесом.

Автоматизоване рішення такого завдання дає можливість грамотно планувати, враховувати витрати, проводити технічну підготовку виробництва, оперативно управляти процесом випуску продукції в відповідності з виробничою програмою і технологією.

Очевидно, що чим більше виробництво, тим більше число бізнес-процесів бере участь у створенні прибутку, а значить, впровадження інформаційних систем спає необхідною складовою компанії.

Управління маркетингом. Управління маркетингом передбачає моделювання параметрів зовнішнього оточення для визначення оптимального рівня цін, прогнозування прибутку і планування рекламних кампаній. Рішення таких систем може бути формалізовано і представлено у вигляді інформаційної системи, що дозволяє істотно підвищити ефективність управління маркетингом.

Документообіг. Документообіг є важливий процес діяльності будь-якого підприємства. Добре налагоджена система облікового документообігу відображає що відбувається на підприємстві і дає керівництву можливість впливати на неї. Тому автоматизація документообігу дозволяє підвищити ефективність управління.

Оперативне управління підприємством. Інформаційна система, яка вирішує завдання оперативного управління підприємством, будується на основі бази даних, в якій фіксується вся можлива інформація про підприємство. Така інформаційна система є інструментом для управління бізнесом і зазвичай називається корпоративною інформаційною системою.

Інформаційна система оперативного управління включає в себе масу програмних рішень автоматизації бізнес-процесів, що мають місце на конкретному підприємстві. Одне з найбільш важливих вимог, що пред'являються до таких інформаційних систем, - гнучкість, здатність до адаптації і подальшого розвитку.

Для побудови КІС використовується архітектура клієнт-сервер, яка отримала визнання і широке поширення як спосіб організації додатків для робочих груп та інформаційних систем корпоративного рівня. Подібна організація роботи підвищує ефективність виконання додатків за рахунок використання можливостей сервера БД, розвантаження мережі і забезпечення контролю цілісності даних [1].

Рис.1.2. Клієнт-серверна архітектура

Дворівневі схеми архітектури клієнт-сервер можуть привести до деяких проблем в складних інформаційних додатках з безліччю користувачів і заплутаною логікою. Рішенням цих проблем може стати використання багаторівневої архітектури.архитектура клиент-сервер получила признание и широкое

распространение как способ организации приложений для рабочих групп и информационных систем корпоративного уровня. Подобная организация работы повышает эффективность выполнения приложений за счет использования возможностей сервера БД, разгрузки сети и обеспечения контроля целостности данных.

1.2. Визначення функцій користувачів корпоративної інформаційної системикористувачі ІС

Будь-яка корпоративна інформаційна система (КІС) повинна забезпечити виконання бізнес процесів компанії. Тому для нормальної роботи КІС необхідно розіміти, які саме користувачі працюють з системою [1]. Згідно виконуваних обов’язків користувачів КІС можна розділити на наступні групи:

випадковий користувач, взаємодія якого з КІС обумовлено службовими обов'язками;

кінцеві користувачі (споживачі інформації) - особа або колектив, в інтересах яких працює КІС. Вони працюють з КІС кожного дня, пов'язані з відповідною областю діяльності і, як правило, вони не є програмістами обо адміністраторами, наприклад, це бухгалтери, економісти, керівники підрозділів;

колектив фахівців (персонал ІС), що включає адміністратора, системного аналітика, системних і прикладних програмістів.

Визначимо більш докладно склад і функції фахівців КІС.

Адміністратор - це фахівець (або група фахівців), який розуміє потреби кінцевих користувачів, працює з ними в тісному контакті і відповідає за визначення, завантаження, захист і ефективність роботи необхідних ресурсів системи. Він повинен координувати процес збору інформації, проектування і підтримки, враховувати поточні та перспективні потреби користувачів [1].

Системні програмісти займаються розробкою і супроводом базового програмного забезпечення ЕОМ (ОС, СУБД, трансляторів, сервісних програм загального призначення).

Прикладні програмісти розробляють програми для реалізації запитів до БД КІС.

Аналітик будує математичну модель предметної області, виходячи з інформаційних потреб кінцевих користувачів; ставить завдання для прикладних програмістів.

Багато співробітників, незважаючи на правила «цифровий гігієни», нехтують вимогами керівництва - відвідують небезпечні або недовірених сайти, відкривають фішингові листи, користуються робочими сервісами через небезпечні Wi-Fi-точки. Тому керівництву компаній необхідно застосовувати серйозні заходи щодо доступу до корпоративної інформаційної системи, як простих користувачів, так і приділяти увагу щодо доступу адміністраторів системи. Не виконуючи таких заходів зловмисники можуть отримувати доступ до привілейованих акаунтів і отримати величезну кількість конфіденційних даних. Складно оцінити збиток від подібних витоків, загальне число вкрадених записів обчислюється мільйонами - інформація про кредитні картки, про співробітників, облікові записи користувачів, медичні записи і багато іншого. Такі атаки і крадіжки даних відбуваються в промислових масштабах. За даними звіту Forrester, 80% ІБ-інцидентів пов'язані з крадіжкою даних привілейованих користувачів, Такі інциденти показують, що хакери можуть вкрасти інформацію завдяки злому привілейованих акаунтів. І це говорить про те, що необхідно звернути увагу на впровадження системи привілейованих користувачів для управління користувачами в КІС.

1.3. Аналіз методів та засобів управління привілейованими користувачами

Привілейовані користувачі - ключ до інформаційної системи. Від їх дій залежить робота інформаційних систем і доступність ресурсів підприємства. Якщо адміністратори зробили помилку або їх облікові дані дістались зловмисникам або конкурентам, це може бути небезпечним для усього бізнесу. А якщо бізнес залежить не від однієї інформаційної системи, а від цілого складного рішення, працездатність якого забезпечується кількома адміністраторами з різними повноваженнями і компетенціями, то проконтролювати їхні дії стає дуже складно і витратно. Особливо якщо в компанії не впроваджена система аутентифікації привілейованих користувачів і всі адміністратори користуються загальним паролем root або admin. Звичайно, якщо всі вони кристально чесні і абсолютно компетентні, то така ситуація ще влаштовувати керівництво, але якщо трапиться інцидент, то буде незрозуміло, кого з них звільняти за некомпетентність.. Тому всіх привілейованих користувачів необхідно розпізнавати окремо і якісно, а також контролювати дії з максимально можливою гранулярністю - аж до конкретних команд, операцій і кнопок в діалогах. Справа в тому, що для зовнішніх зловмисників можливість підробитися під адміністратора і є методом повного захоплення інформаційної системи. Тому надійність механізму аутентифікації адміністраторів та інших привілейованих користувачів є ключем до всієї системи безпеки компанії [2].

Згідно аналітики Gartner виділено конкретні чинники, що впливають на зростання ринку щодо впровадження систем управління привілейованими користувачами PAM включають:

• Організації, які прагнуть знизити ризик зломів і внутрішніх загроз, які часто пов'язані з вкраденими, скомпрометовані або неправомірно використаними привілейованими обліковими даними.

• Зростаюче число нормативних вимог і нормативних вимог, які вимагають, явно чи неявно, контролю над привілейованими користувачами і захисту привілейованих облікових даних.

• Невдалі аудити, оскільки аудитори продовжують розуміти важливість контролю і моніторингу активності привілейованих користувачів і посилаються на відсутність або неадекватність таких засобів контролю в якості висновків.

• Раптовий перенесення віддаленої роботи для привілейованих користувачів через пандемію COVID-19.

До інших чинників, що сприяють розширенню використання інструментів PAM, відносяться:

• Необхідність надавати і контролювати привілейований доступ третім сторонам, таким як постачальники, підрядники, постачальники послуг і бізнес-партнери, що призвело до поширення використання функцій віддаленого привілейованого доступу з інструментів PAM.

• Розвиток можливостей PAM для управління всіма типами секретів в середовищі організації.

• Бажання підвищити ефективність роботи адміністраторів і операторів.

• Забезпечення підтримки загальної стратегії кібербезпеки.

Саме для PAM Gartner визначив основні допущення стратегічного планування кібербезпеки компаній.

До 2024 року 50% організацій будуть впроваджувати модель привілейованого доступу «точно в строк» (JIT), яка усуває постійні привілеї, і на 80% зменшує порушення привілеїв, ніж у тих, які цього не роблять.

До 2024 року 65% організацій, що використовують функції автоматизації привілейованих завдань, заощадять 40% витрат на персонал для IT-операцій для IaaS і PaaS і отримають на 70% менше порушень, ніж ті, які цього не роблять.

Gartner визначає ринок управління привілейованим доступом (PAM) як інструменти, які пропонують одну або декілька з наступних функцій:

• Виявлення, управління і управління привілейованими обліковими записами (облікові записи з привілеями суперкористувача / адміністратора) в декількох системах і додатках.

• Керування доступом до привілейованих облікових записів, включаючи загальний та аварійний доступ.

• Випадкова зміна, управління і зберігання облікових даних (пароль, ключі і т. д.) Для облікових записів адміністраторів, служб і додатків.

• Забезпечення єдиного входу (SSO) для привілейованого доступу, щоб запобігти розкриттю облікових даних.

• Відстеження, фільтрація і координація привілейованої команди, дії і завдання.

• Управління обліковими даними додатків, служб і пристроїв і відправка їх посередникам, щоб уникнути викриття.

• Моніторинг, запис, аудит і аналіз привілейованого доступу, сеансів і дій.

Gartner охоплює три окремі категорії інструментів, які стали основним напрямком діяльності фахівців з безпеки та управління ризиками (SRM) і інших IT-лідерів, що розглядають можливість інвестування в інструменти PAM:

• *Привілейований аккаунт і управління сесіями (PASM).* 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) встановлюють сеанси з можливим введенням облікових даних і повнимим записом сеансу. Паролі та інші облікові дані для привілейованих облікових записів активно управляються, наприклад змінюються через певні інтервали або при виникненні певних подій. Рішення PASM можуть додатково забезпечувати управління паролями між додатками (AAPM) і / або функції віддаленого привілейованого доступу з нульовою установкою для IT-персоналу і третіх осіб, яким не потрібно VPN.

• *Управління підвищенням привілеїв і делегуванням (PEDM).* У керованій системі агенти хоста надають певні привілеї користувачам, які увійшли систему. Інструменти

PEDM забезпечують управління командами (фільтрацію) на основі хоста, дозволяють / забороняють / ізолюють елементи управління додатками і / або підвищують привілеї, причому останнє в формі дозволу виконання певних команд з більш високим рівнем привілеїв. Інструменти PEDM повинні виконуватися в реальній операційній системі (на рівні ядра або процесу). Командне управління через фільтрацію протоколу явно виключено з цього визначення, оскільки точка управління менш надійна. Інструменти PEDM можуть додатково надавати функції моніторингу цілісності файлів.

• *Управління секретами:* облікові дані (такі як паролі, токени OAuth, ключі SSH і т. д.) і секрети для програмного забезпечення і комп'ютерів управляються програмно, зберігаються і отримуються через API і 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.

Розглянемо магічний квадрант Gartner, де включено постачальників, які надають повністю функціональний продукт PASM (Рис.1.2).

Розглянемо деякі з рішень PAM, для визначення найкращого рішення для розробки майбутніх рекомендацій.

Рис.1.2 Магічний квадрант Gartner продуктів PASM

ARCON

ARCON - претендент в цьому магічному квадраті; в останній ітерації цього дослідження це був нішевий гравець.

Його продукт ARCON Privileged Access Management поставляється у вигляді пристрою, програмного забезпечення або SaaS і забезпечує можливості зберігання і управління сеансами (PASM), а також функції PEDM для Windows і UNIX / Linux. ARCON продовжує вкладати значні кошти в аналітику, пропозиції SaaS і в підвищення масштабованості свого рішення.

Сильні сторони:

• Підтримка: постачальник не робить відмінностей між різними рівнями технічної підтримки. Він пропонує цілодобову підтримку для всіх клієнтів в якості основного надання допомоги. Вартість підтримки заснована на процентному співвідношенні витрат на ліцензію, який становить 18%, що значно нижче ставок інших постачальників.

BeyondTrust

BeyondTrust - лідер в цьому магічному квадраті; в останній ітерації цього дослідження це був Лідер.

Він пропонує можливості PASM з Password Safe в якості програмного забезпечення або пристрою, а також Cloud Vault через SaaS. Можливості PEDM надаються через Управління привілеями для Windows і Mac і управління привілеями для UNIX і Linux.

Сильні сторони

• Продукт: BeyondTrust пропонує рішення під назвою Privileged Remote Access (PRA), яке надає зріле і просте в розгортанні рішення для підтримки адміністраторів (включаючи сторонніх користувачів), яким потрібно віддалений привілейований доступ.

Broadcom (Symantec)

Symantec є нішевим гравцем в цьому «Магічному квадраті»; в останній ітерації цього дослідження він був лідером (що має назву CA Technologies).

Частина рішення PASM надається Symantec Privileged Access Manager, доступним у вигляді захищеного пристрою або віртуального образу. Послуги PESM надаються продуктом управління сервером Privileged Access Manager, заснованим на агентах. Також доступні агенти AAPM.

Сильні сторони

• Продукт: Privileged Access Manager має дуже ефективні і масштабовані можливості PSM, які можуть обробляти більше одночасних підключень, ніж більшість інших оцінюваних товарів.

• Продукт: Рішення має широкий спектр підтримки PEDM для Windows і UNIX / Linux з відмінним набором функцій, включаючи моніторинг цілісності файлів.

• Продукт: рішення має безліч функцій корпоративного рівня, таких як спеціальний драйвер підключення до бази даних Java (JDBC) для управління підключенням до бази даних, що зазвичай не зустрічається в інших рішеннях, і унікальна підтримка JIT-фільтрації Amazon Web Services (AWS) і WAN-кластеризація на основі.

Centrify

Centrify - лідер в цьому магічному квадраті; в останній ітерації цього дослідження це був Лідер.

Його рішення Centrify Privileged Access Service в основному орієнтовано на PASM на основі SaaS, тоді як Centrify Privilege Elevation Service має можливості PEDM. Centrify також пропонує підтримку UNIX / Linux та Active Directory (AD) через Centrify Authentication Service.

Сильні сторони

• Продукт: Centrify включає в себе повне рішення віддаленого привілейованого доступу на основі SaaS, в якому немає необхідності встановлення клієнта на програмному забезпеченні, такому як рішення VPN.

• Якість обслуговування клієнтів: управління доступне в Інтернеті без реєстрації. Крім того, Centrify пропонує безкоштовну послугу Centrify Health Check - одноденну консультаційну програму для оцінки зрілості програми PAM і визначення наступних кроків.

• Продукт: Centrify пропонує зрілу і багатофункціональну можливість моста AD для UNIX / Linux, яка включає такі функції, як моніторинг цілісності файлів, як частина служби підвищення привілеїв.

• Стратегія продукту: у Centrify є хороша дорожня карта з сильним конвеєром для нових функцій. Варіанти розгортання і ліцензування різноманітні, гнучкі і включають в себе хмарні, локальні і SaaS-рішення.

CyberArk

CyberArk - лідер в цьому магічному квадраті; в останній ітерації цього дослідження це був Лідер.

Його рішення Privileged Access Security (PAS) пропонує можливості PASM у вигляді програмного забезпечення або SaaS. Для PEDM CyberArk пропонує диспетчер привілеїв кінцевих точок (EPM) для Windows і Mac і диспетчер привілеїв на вимогу (OPM) для UNIX / Linux. Application Access Manager пропонує управління секретами. CyberArk має географічну диверсифікацію. У травні 2020 року CyberArk розширилася до управління доступом, придбавши Idaptive.

Сильні сторони

• Успіх на ринку PAM: CyberArk має давню історію на ринку PAM, і цей бренд дуже добре відомий. Майже всі клієнти Gartner, які вивчають продукти PAM, включають CyberArk в свій список постачальників для оцінки.

• Стратегія продукту: CyberArk володіє широким набором можливостей для обслуговування переважної більшості потреб PAM. Набір продуктів дуже зрілий і може працювати зі складними сценаріями і крайніми випадками.

• Інновації: CyberArk має історію передових інновацій; У минулому році компанія розробила нового «бессекретного» брокера для розширення можливостей

свого інструменту управління секретами і повноцінного вирішення віддаленого привілейованого доступу на основі SaaS під назвою Alero, що зробило непотрібним встановленняя замовником програмного забезпечення для віддаленого доступу, таке як рішення VPN.

Hitachi ID Systems

Hitachi ID Systems - претендент в цьому «магічному квадраті»; в останній ітерації цього дослідження це був нішевий гравець.

Його програмний продукт Privileged Access Manager (HIPAM) орієнтований на PASM і може бути розгорнутий в центрах обробки даних або в приватних хмарах AWS.

Сильні сторони

• Продукт: рішення має відмінні можливості виявлення, управління обліковими даними і автоматизації. Крім того, він має безліч додаткових корисних функцій, які зазвичай не зустрічаються в конкуруючих продуктах PAM, таких як зіставлення і аналіз довіри ключів SSH або можливість очищення конфіденційних даних із записів.

Krontech

Krontech є нішевим гравцем в цьому «Магічному квадраті».

Його інструмент Single Connect поставляється у вигляді програмного забезпечення та орієнтований на можливості PASM, включаючи обмежену функціональність PEDM UNIX / Linux. Його діяльність в основному зосереджена в Європі і Північній Америці.

Сильні сторони

• Продукт: Krontech йде далі, ніж інші постачальники PAM, в підтримці великих засобів фільтрації SQL і маскування даних для моніторингу та управління привілейованим доступом до бази даних.

• Продукт: Single Connect забезпечує повне оптичне розпізнавання символів (OCR) для захоплених графічних сеансів, дозволяючи аудиторам шукати артефакти, які відображаються на екранах під час активності, які інакше було б важко знайти.

• Продукт: Single Connect розроблений для використання у великих середовищах і з добре масштабуємою архітектурою, яка підтримує масову паралельну ротацію облікових даних.

• Інновація: Krontech розробив для свого рішення функцію мультіарендності. Це дає замовнику можливість надавати PAM як послугу для різних груп, яким потрібні послуги PAM, всередині або поза компанією, але з ізоляцією між цими групами.

WALLIX

WALLIX - нішевий гравець в цьому «Магічному квадраті»; в останній ітерації цього дослідження це був нішевий гравець.

Лінія продуктів WALLIX Bastion доступна як програмне забезпечення або як пристрій (віртуальне або фізичне), орієнтоване на PASM. Можливості AAPM і PEDM для Windows також доступні у вигляді програмного забезпечення. Діяльність WALLIX в основному зосереджена в країнах Європи, Близького Сходу і Африки та Північної Америки.

Сильні сторони

• Продукт: WALLIX Bastion може забезпечувати повне розпізнавання тексту для захоплених графічних сеансів, дозволяючи аудиторам шукати артефакти, які відображаються на екранах під час активності, які інакше було б важко знайти.

• Продукт: На відміну від більшості інших постачальників, які вимагають, щоб вразливі ключі API зберігалися додатками, AAPM постачальника використовує комплексну ідентифікацію додатків на основі агентів. Цей метод може ефективно видалити будь-які статичні облікові дані з додатків або сценаріїв.

• Галузева стратегія: WALLIX пропонує з'єднувачі для певних промислових систем управління і операційних систем.

Таким чином для подальшої роботи будемо досліджувати методи та засоби управління привілейованими користувачами на базі рішення CyberArk.

2 МЕТОДИ ТА ЗАСОБИ РЕАЛІЗАЦІ СИСТЕМИ УПРАВЛІННЯ ПРВІЛЕЙОВАНИХ КОРИСТУВАЧІВ НА БАЗІ CYBERARK

2.1. Життевий цикл системи управління привілейованих користувачів

Багато компаній все більше і більше стурбовані постійно мінливим ландшафтом загроз кібератак, спостерігаючи, як великі відомі корпоративні організації стають жертвами кіберзлочинів. Щорічно крадуть мільярди записів, збільшується кількість випадків крадіжки особистих даних, збільшується кількість випадків зловживання обліковими даними, а фінансове шахрайство досягає мільярдів доларів.

Для захисту від кіберзлочинів вже недостатньо покладатися лише на технології. Однією традиційної безпеки вже недостатньо .

Традиційна кібербезпека більше не є стійкою. Це занадто складно, часто занадто складно управляти і, як наслідок, занадто дорого - як за часом, так і по грошах. Таким чином, у організацій не має іншого вибору, окрім як прискорити перехід до більш простих рішень, які знімають складні управлінські вимоги до IT-персоналу і в той же час створюють більш безпечні і плавні інтеграції.

Кібербезпека привілейованого доступу в даний час є одним з головних засобів управління безпекою, якому багато керівників з інформаційної безпеки приділяють пріоритетну увагу, щоб допомогти їм знизити ризики кібератак, розширити можливості своїх співробітників і захистити свої організації від несанкціонованого доступу.

Попередній досвід роботи з успадкованими постачальниками рішень для управління привілейованими обліковими записами був складним, вимагав дорогих фахівців, був дуже дорогим, на впровадження йшли роки або ніколи не встановлювали повністю.

Організації, які тільки починають працювати з захистом і забезпеченням привілейованого доступу, повинні визначити, які привілейовані облікові записи повинні бути, а також переконатися, що ті, хто буде використовувати ці привілейовані облікові записи, чітко розуміють прийнятне використання і відповідальність.

Перед реалізацією стратегії управління привілейованим доступом необхідно визначити, що таке привілейований обліковий запис для організації. У кожній компанії все по-різному, тому дуже важливо визначити, які важливі бізнес-функції залежать від даних, систем і доступу.

Отже, що означає привілейований доступ у організації? Це може означати доступ до інфраструктури, конфіденційних даних, налаштування систем, розгортання виправлень, сканування на уразливості, хмарні середовища і багато іншого. Щоб отримати чітке визначення, необхідно виконати оцінку впливу на дані, тому що це саме те, що захищає і використовується більшістю привілейованих облікових записів - для доступу до конфіденційних даних або забезпечення доступу до конфіденційних даних.

Після того, буде проведено оцінку впливу на дані для класифікації своїх даних, буде отримано, яка інформація найбільш важлива для вашого бізнесу.

Потім необхідно перевірити і підтвердити, хто повинен мати права доступу для перегляду цих конфіденційних даних і управляти ними.

Привілейовані облікові записи можуть бути людськими або нелюдськими. Деякі привілейовані облікові записи пов'язані з окремими особами, такими як бізнес-користувачі або мережеві адміністратори, в той час як інші є обліковими записами додатків, що використовуються для запуску служб, і не пов'язані з унікальною особистістю людини.

Після оцінку впливу на дані, наступним кроком до зрілості буде дотримання життєвого циклу привілейованого доступу.tic. Це допоможе швидко просунутися по шляху захисту і захисту привілейованого доступу.

Рис.2.1. Життєвий цикл PAM

Кроки життєвого циклу PAM:

Визначати

Визначити і класифікуйте привілейовані облікові записи. Кожна організація індивідуальна, тому необхідно визначити, які важливі бізнес-функції залежать від даних, систем і доступу. Переконатися, що узгодили привілейовані облікові записи з бізнес-ризиками і операціями.

Надалі необхідно розробити політики безпеки IT, які явно охоплюють привілейовані облікові записи. Багато організацій як і раніше не мають прийнятного використання і відповідальності за привілейовані облікові записи.

Виявити

Відкрийте для себе свої привілейовані облікові записи. Використовуйте автоматизоване програмне забезпечення PAM для ідентифікації привілейованих облікових записів і реалізуйте безперервне виявлення, щоб обмежити розростання привілейованих облікових записів, виявити потенційні внутрішні зловживання і

виявити зовнішні загрози. Це допоможе забезпечити повну і постійну видимість ландшафту вашого привілейованого облікового запису, який має вирішальне значення для боротьби з загрозами кібербезпеки.

Керувати і захищати

Необхідно забезпечити захист паролів своїх привілейованих облікових записів. Проактивно керуйте, відстежуйте і контролюйте доступ до привілейованих облікових записів за допомогою програмного забезпеченняя захисту пароля. Обране рішення має автоматично виявляти і зберігати привілейовані облікові записи; запланувати ротацію паролів; аудит, аналіз і управління окремими привілейованими сеансами; і відстежувати паролі облікових записів, щоб швидко виявляти шкідливі дії і реагувати на них.

Необхідно обмежити доступ IT-адміністратора до систем. Розробити політику мінімальних привілеїв, щоб привілеї надавалися тільки в разі потреби і затвердження. Забезпечити мінімальні привілеї на кінцевих точках, зберігши для кінцевих користувачів стандартний профіль користувача і автоматично підвищуючи їх права для запуску тільки затверджених і довірених додатків. Для користувачів з привілейованими обліковими записами IT-адміністраторів необхідно контролювати доступ і впроваджувати управління супер-повноваження для систем Windows і UNIX, щоб запобігти запуск зловмисниками шкідливих додатків, інструментів і команд віддаленого доступу. Рішення з мінімальними привілеями та контролем додатків дозволять без проблем підвищувати рівень схвалених, довірених і внесених в білий список додатків, зводячи до мінімуму ризик запуску неавторизованих додатків.

Моніторинг

Рішення PAM має можливість відстежувати і записувати активність привілейованої облікового запису. Це допоможе забезпечити належну поведінку та уникнути помилок співробітників та інших IT-користувачів, оскільки вони знають, що їх дії відстежуються. Якщо порушення дійсно відбудеться, моніторинг використання привілейованого облікового запису також допоможе цифровий криміналістиці

визначити основну причину і виявити важливі елементи управління, які можна покращити, щоб знизити ризик майбутніх загроз кібербезпеки.

Виявлення ненормального використання

Відстежуйте і попереджайте про поведінку користувачів. Оскільки до 80% порушень пов'язані зі зламаним користувачем або привілейованого облікового запису, отримання інформації про доступ до привілейованого облікового запису і поведінці користувачів є головним пріоритетом. Забезпечення прозорості доступу і активності ваших привілейованих облікових записів в режимі реального часу допоможе виявити підозрювану компрометацію облікового запису і потенційні зловживання з боку користувачів. Поведінкова аналітика фокусується на ключових точках даних для визначення індивідуальних базових показників користувача, включаючи активність користувачів, доступ по паролю, аналогічна поведінка користувачів і час доступу для виявлення і попередження про незвичайну або ненормальну активность.

Реагування на інциденти

Підготуйте план реагування на інциденти на випадок злому привілейованого облікового запису. Коли обліковий запис зламано, проста зміна паролів привілейованої облікового запису або відключення привілейованої облікового запису неприпустимо. У разі злому хакери можуть встановити шкідливе ПЗ і навіть створити свої власні привілейовані облікові записи.

Аналіз та аудит

Постійне спостереження за використанням привілейованих облікових записів за допомогою аудитів та звітів допоможе виявити незвичайну поведінку, яка може вказувати на порушення або неправильне використання. Ці автоматичні звіти також допомагають відстежити причину інцидентів безпеки, а також продемонструвати дотримання політик і правил. Аудит привілейованих облікових записів також надасть показники кібербезпеки, які нададуть керівництву життєво важливу інформацію для прийняття більш обгрунтованих бізнес-решень.

2.2. Обгрунтування принципів рішення Privileged Access Security

Рішення Privileged Access Security забезпечить кібербезпеку компанії, де всі адміністративні паролі можуть бути надійно заархівовані, передані і надані авторизованим користувачам, таким як IT-персонал, чергові адміністратори і локальні адміністратори у віддалених місцях.

Множинні рівні безпеки (включаючи брандмауер, VPN, аутентифікацію, контроль доступу, шифрування і ін.), які лежать в основі рішення Privileged Access Security, та пропонують найбільш безпечне рішення для зберігання та обміну паролями в корпоративному середовищі.

Рішення Privileged Access Security - це рішення plug-and-play, яке вимагає мінімальних зусиль для налаштування і яке може бути повністю готове до роботи за дуже короткий період часу. Доступ до нього і управління ним можна отримати за допомогою клієнта Windows, веб-інтерфейсу або різних API-інтерфейсів.

На рис. 2.2 показані різні компоненти рішення Privileged Access Security і їх взаємодія.

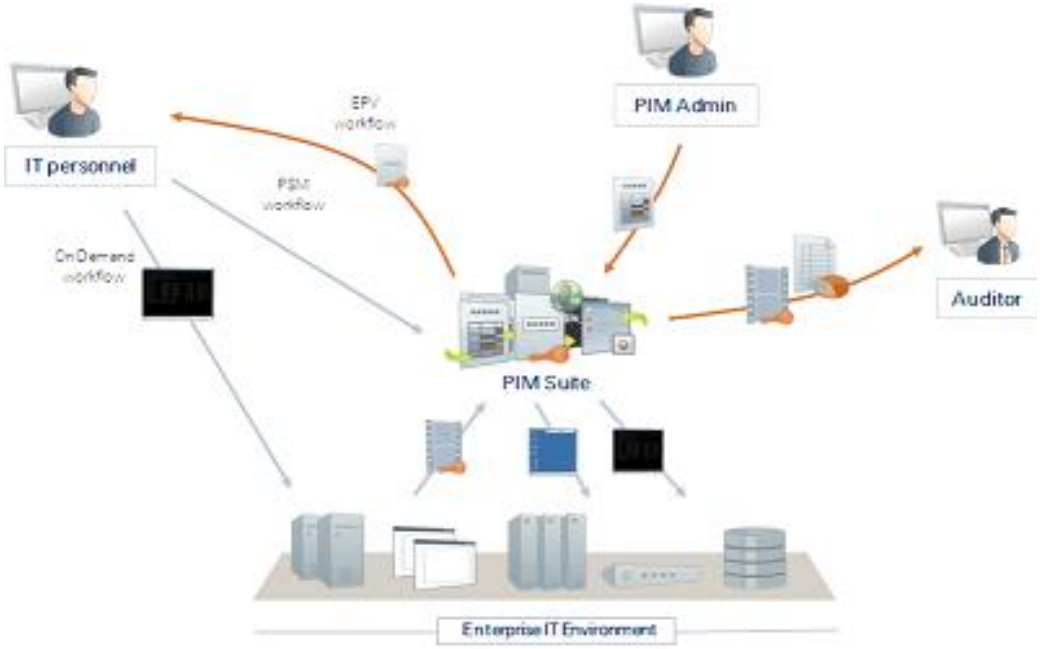

Рис.2.2. Архітектура рішення безпеки привілейованого доступа

Архітектура рішення Privileged Access Security складається з двох основних елементів. Одним з них є Storage Engine (так званий «сервер» або просто «сховище»), який зберігає дані і відповідає за захист даних в стані спокою і забезпечення аутентифицированного і контрольованого доступу.

Другий елемент - це інтерфейс (інтерфейси Windows, веб-інтерфейси і SDK), який взаємодіє з Storage Engine, з одного боку, і надає доступ користувачам і додаткам, з іншого. Storage Engine і інтерфейс обмінюються даними за допомогою безпечного протоколу CyberArk - протоколу Vault.

Визначення комплексної стратегії PAM є критичним кроком у визначенні ключових ризиків, які необхідно знизити в компанії, і у визначенні пріоритетів діяльності програми. Ця стратегія, як правило, заснована на поєднанні інфраструктури кібербезпеки компанії, виникаючих загроз, галузевих тенденцій і вимог до нагляду. Надійна стратегія PAM дозволяє розробити план зниження ризиків, дорожню карту для привілейованого доступу і цільову операційну модель (ЦОМ), які допомагають забезпечити довгострокову стійкість засобів контролю.

Рис2.3. Схема стратегії зниження ризиків PAM

Розробка моделі PAM не тільки дає довгострокове уявлення про розроблену стратегію зниження ризиків, але також дозволяє розглядати короткострокові швидкі

вигоди, такі як надання засобів управління PAM, які забезпечують швидке зниження ризиків з найменшими зусиллями.

Розглянемо принцип CyberArk Blueprint для успішного управління привілейованим доступом більш детально (рис2.4. та 2.5)

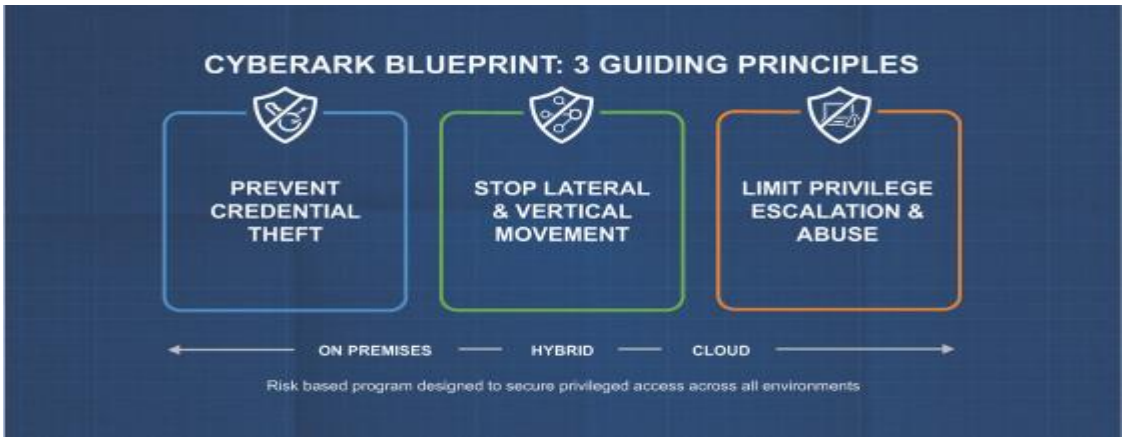

Рис.2.4. Принцип CyberArk Blueprint для успішного управління привілейованим доступом

Рис. 2.5. Квадрант методології пріорітізації ріcків, CyberArk Blueprint

Проект CyberArk для успішного управління привілейованим доступом базується на трьох керівних принципах [4]:

1. Запобігання крадіжці облікових даних. Паролі та ключі іноді залишаються незмінними протягом місяців чи навіть років після їх видачі. Колишні співробітники, підрядники та бізнес-партнери часто зберігають доступ до критичних програм та систем довгий час після припинення їхдії, піддаючи бізнес порушенням даних та проведення зловмисних атак. Незадоволені співробітники або зовнішні зловмисники можуть використовувати неактивні акаунти або застарілі паролі для здійснення складних атак.

Рис. 2.6. Принцип крадіжки облікових даних

2. Зупинка горизонтального та вертикальнго руху. Маючи в наявності облікові дані, супротивник часто переходить від систем нижчої вартості до цілей вищої вартості, що містять більш важливу інформацію або може використати для управління середовищем компанії. Це може відбуватися у наступних формх: 1. Переміщення горизонтально, в межах того самого "рівня ризику" в надії знайти кращі, корисніші дані. 2. Перехід по вертикалі від одного рівня ризику до іншого (наприклад, перехід від робочих станцій до серверів), щоб наблизитись до більш цінної інформації.

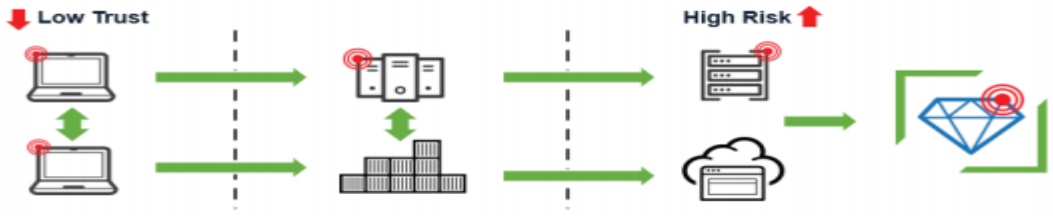

Рис.2.7. Принцип горизонтального та вертикального руху ризику

3. Обмеження ескалації та зловживаннями привілеями. Привілейовані акаунти є широко поширеними. Кожен хост, додаток, база даних та платформа мають власні вбудовані адміністративні дані. Багато організацій адмініструють привілейовані облікові дані вручну і мають обмежену видимість та контроль над привілейованими сеансами. І, що ще гірше, багато організацій надмірно привілеюють кінцевих користувачів та процеси подання заявок, надаючи їм повноцінні дані права адміністратора, незалежно від їх фактичних вимог. Поширення привілейованих рахунків та відсутність адміністративної видимості і контроль створюють широку поверхню атаки для використання інсайдерами та зовнішніми зловмисниками.

Для того щоб захистити свої організаційні привілеї, важливо розуміти поточний стан привілеїв на вашому підприємстві. Це включає в себе інвентаризацію активів у вашому операційному середовищі і масиві привілейованих облікових записів, які використовуються для їх підтримки. Привілейовані облікові записи та облікові дані можна знайти всюди - включаючи Active Directory, * NIX, IaaS, PaaS, SaaS, SQL і багато інших IT і бізнес-сервіси. Важливо часто сканувати системи у мережі і постачальників хмарних послуг для виявлення привілейованих облікових записів, облікових даних, прав і неправильних конфігурацій, які можуть спричинити небезпеку для організації.

Дані, отримані в процесі інвентаризації, дозволяють оцінити рівень ризику на основі структури PAM і встановити набір цілей і пріоритетів для графіка впровадження.

Один з кращих способів - інтегрувати дане рішення PAM з технологіями управління та виявлення вразливостей від таких постачальників, як Rapid7, Forescout і Tenable. Це забезпечує безпеку привілейованих облікових даних, які використовуються для автоматичного входу в уразливі середовища інфраструктури.

Розглянеми підхід організації доступа «application-by-application», який включає в себе захист усіх елементів людських та нелюдських привілеїв для одного додатка.

Корпоративні додатки, як правило, знаходяться на кількох платформах (віртуалізація, домен, ОС, база даних і т. д.), а для захисту додатків необхідно визначити кожну привілегію цього додатка. Такий підхід досить складний і результатисвний. Однак на практиці це поганий підхід для забезпечення загальної безпеки. Виявлення для всіх рівнів платформи може зайняти багато часу і не обов'язково зможе запобігти іншим методам входу в додаток. Тому платформний підхід, який починається з віртуалізації і привілеїв на рівні домену, забезпечує основу, на якій знаходяться всі додатки. Крім того, зосередження уваги на захисті технологічної платформи забезпечує економію на масштабі і підвищення ефективності щодо виявлення, оцінки та адаптації (Рис 2.8.).

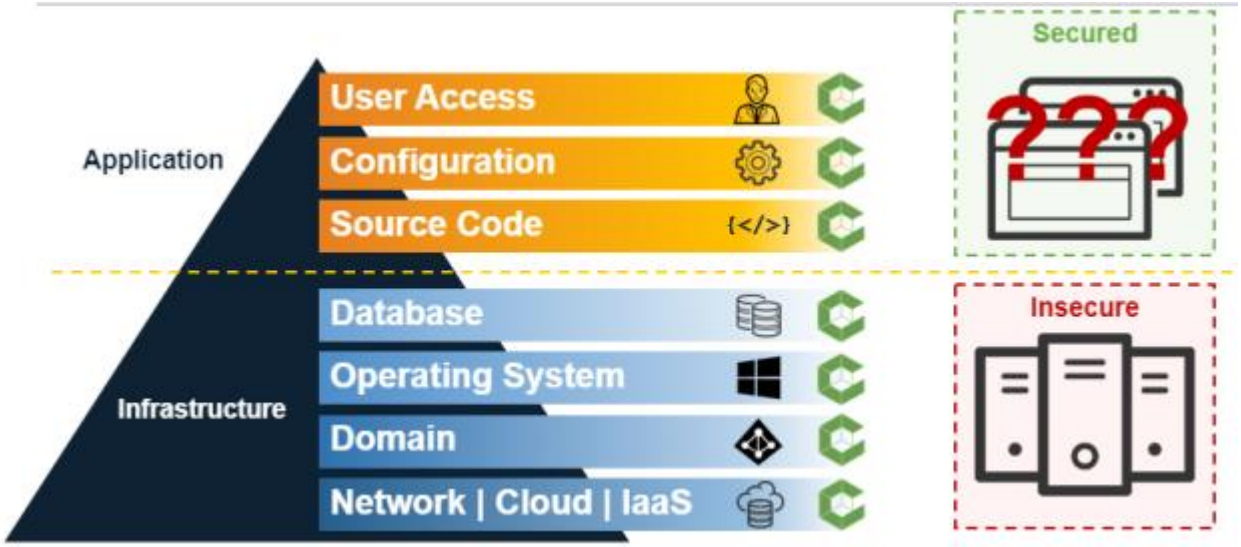

Рис. 2.8. Платформенний підхід до призначення привілеїв доступу

Таким чином визначивши принципи до управління доступом привілейованих користувачів, перейдоме до визначення архітектури та основних функціональних модулів CyberArk Privileged Account Security.

2.3. Склад модулів CyberArk Privileged Account Security

Система управління привілейованими обліковими записами CyberArk Privileged Account Security Solution - рішення корпоративного класу, орієнтоване на великі центри обробки даних (локальні і хмарні), а також на OT / SCADA-середовища. Рішення є комплексним і включає в себе ряд модулів [5, 6]:

Enterprise Password Vault-забезпечує захист, управління і контроль доступу до привілейованих облікових записів;

Privileged Session Manager - забезпечує ізоляцію, контроль і моніторинг доступу привілейованих користувачів, а також контроль дій щодо будь-яких захищених систем - без обмежень типів систем або протоколів;

SSH Key Manager - забезпечує захист, управління і контроль доступу до SSH-ключів;

Privileged Threat Analytics - здійснює аналіз поведінки привілейованих користувачів і оповіщає про потенційно небезпечні дії, що дозволяє оперативно відреагувати і перервати проходження атаки;

Application Identity Manager - здійснює захист, управління і аудит вбудованих привілейованих облікових записів, які використовуються додатками для доступу до підключених систем;

CyberArk Viewfinity-управляє привілеями користувачів і додатками на кінцевих пристроях Windows;

On-Demand Privileges Manager-забезпечує управління і безперервний моніторинг команд, які виконуються на кінцевих * NIX-пристроях. Кожен модуль є автономним і може функціонувати незалежно від інших.

Таким чином, робота всіх модулів разом забезпечує закінчене комплексне рішення для управління привілейованими користувачами (рис.2.9).

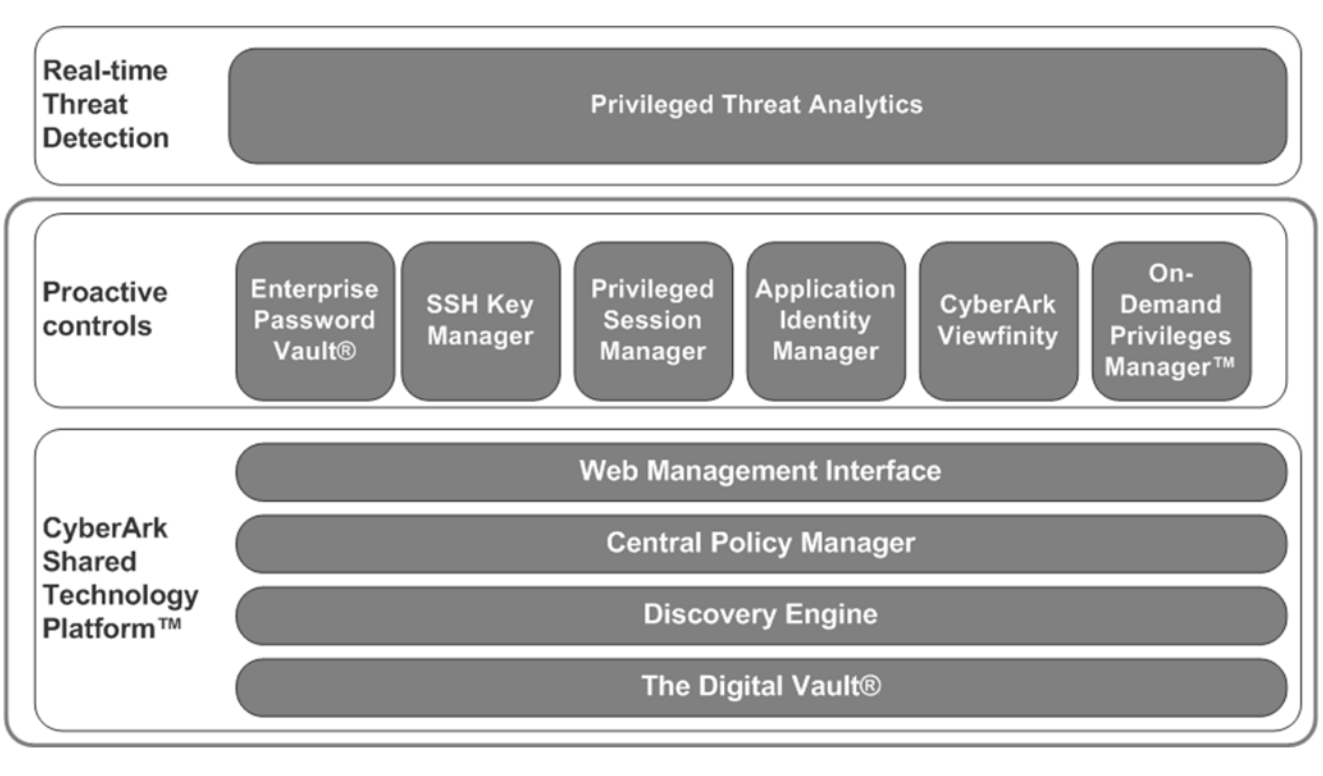

Рис.2.9. Склад модулів CyberArk Privileged Account Security

Основними (базовими) і найбільш затребуваними на ринку є модулі Enterprise Password Vault і Privileged Session Manager, тому надалі більш детально їх розглянемо.

«Ядром» системи CyberArk є Privileged Account Security яка є модульною платформою CyberArk Shared Technology Platform. На базі модульної платформи побудовані всі компоненти CyberArk Privileged Account Security Solution.

Платформа включає:

Digital Vault -захищене цифрове сховище облікових даних, політик і захищаються файлів зібраної доказової бази. Компонент встановлюється на виділений сервер і працює в вигляді сервісу;

Discovery Engine - засоби автоматичного виявлення привілейованих акаунтів в IT-інфраструктурі.

Central Policy Manager - єдиний механізм управління політиками доступу, акаунтами, подіями безпеки і процесами узгодження надання доступу;

Web Management Interface - механізм управління компонентами системи через веб-інтерфейс, надає єдину точку входу, як для користувачів цільових систем, так і для адміністраторів і аудиторів системи CyberArk [6].

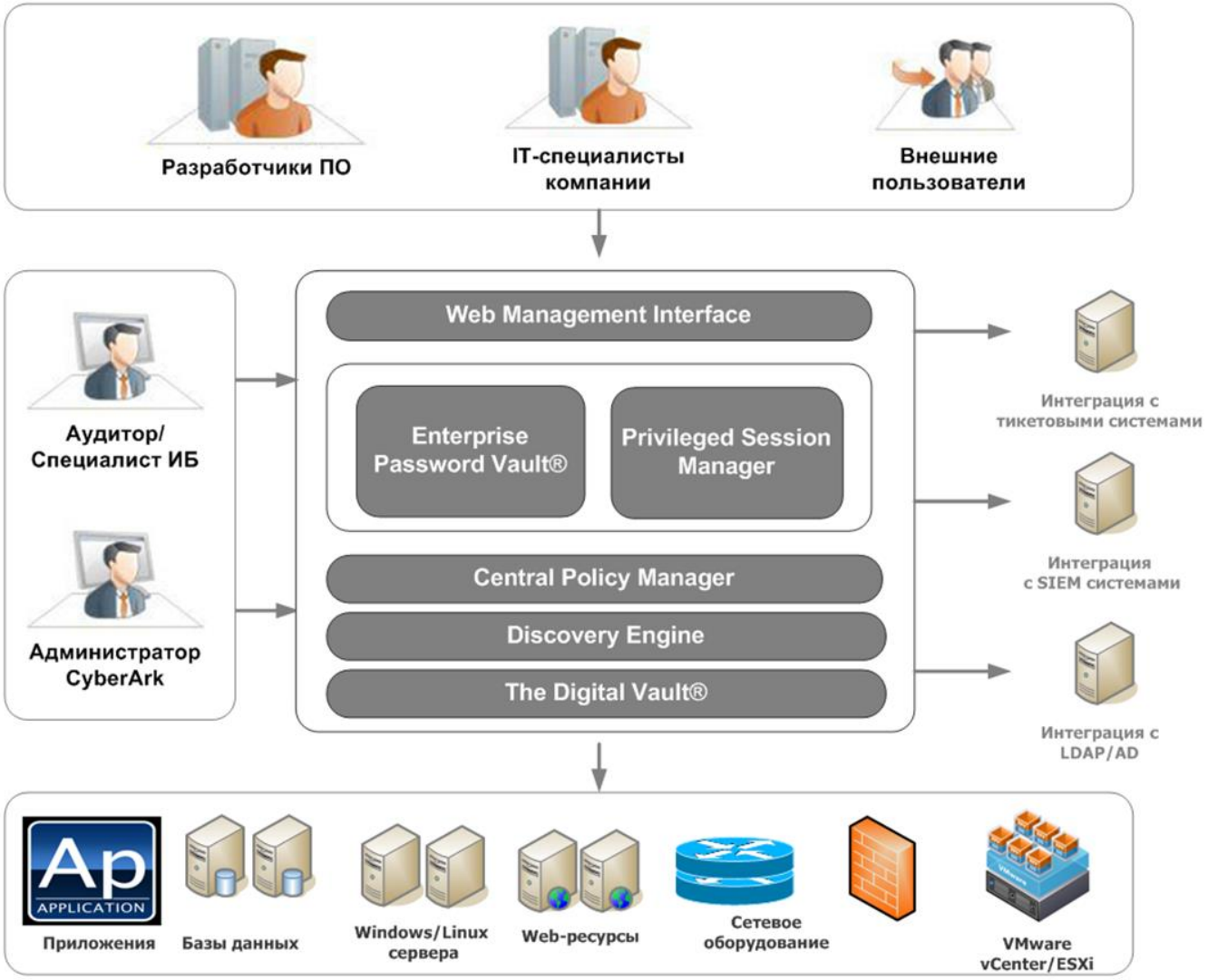

Рис.2.10. Архітектура рішення

Enterprise Password Vault надає сервіс управління життєвим циклом паролів на будь-яких цільових системах: додатки, бази даних, Windows / Linux системи і ін.

Enterprise Password Vault дозволяє захищати, керувати, автоматично змінювати паролі і зберігати логи всіх дій з усіма типами привілейованих облікових записів.

Робота з Enterprise Password Vault здійснюється через веб-інтерфейс Password Vault Web Access.

Privileged Session Manager забезпечує повну ізоляцію систем IT-середовища компанії від осіб, які не наділених відповідними повноваженнями на доступ. Privileged Session Manager функціонує у вигляді Jump-сервера - трафік не перенаправляється, а відкривається незалежна сесія, що дозволяє ізолювати системи від прямого доступу. Це основна відмінність CyberArk Privileged Account Security від інших систем класу PUM / PAM, що використовують проксі-сервер і перенаправляють мережевий трафік до кінцевих систем. Робота з Privileged Session Manager здійснюється через веб-інтерфейс Password Vault Web Access.

Рішення CyberArk Privileged Account Security Solution має «безагентскую» архітектуру - не вимагає розгортання агентів захисту на кінцевих системах.

CyberArk Privileged Account Security Solution також підтримує інтеграцію з наступними типами систем: з системами класу SIM / SIEM, що дозволяє вбудувати продукт в загальну інфраструктуру інформаційної безпеки організації; з тікет-системами, що дозволяє обробляти запити на доступ через них; з системами LDAP / Active Directory, що дозволяє використовувати доменні облікові записи.

Розглянемо етапи процесу роботи з CyberArk Privileged Account Security Solution [6] .

Етапи роботи з модулями Enterprise Password Vault і Privileged Session Manager в архітектурі CyberArk Privileged Account Security Solution виглядає наступним чином: Етап 1.Користувач проходить процедури ідентифікації / аутентифікації на порталі Password Vault Web Access, створює запит на з'єднання з кінцевої системою.

Етап 2. Після узгодження запиту на з'єднання користувач з'єднується з сервером Privileged Session Manager по протоколу RDP і отримує аутентифікаційні дані зі сховища.

Етап 3. Після аутентифікації сервер Privileged Session Manager з'єднує користувача безпосередньо з кінцевої системою нативним протоколом.

Етап 4. Під час сесії користувача ведеться безперервний запис дій, виконуваних на керованих пристроях. Запис ведеться в відео-форматі (для графічних сеансів) і в текстовому форматі (для сеансів командного рядка).

Етап 5. Записи зберігаються в сховищі і доступні аудиторам і фахівцям з інформаційної безпеки для перегляду та аналізу. Можлива відправка подій безпеки в системи SIM / SIEM / Syslog.

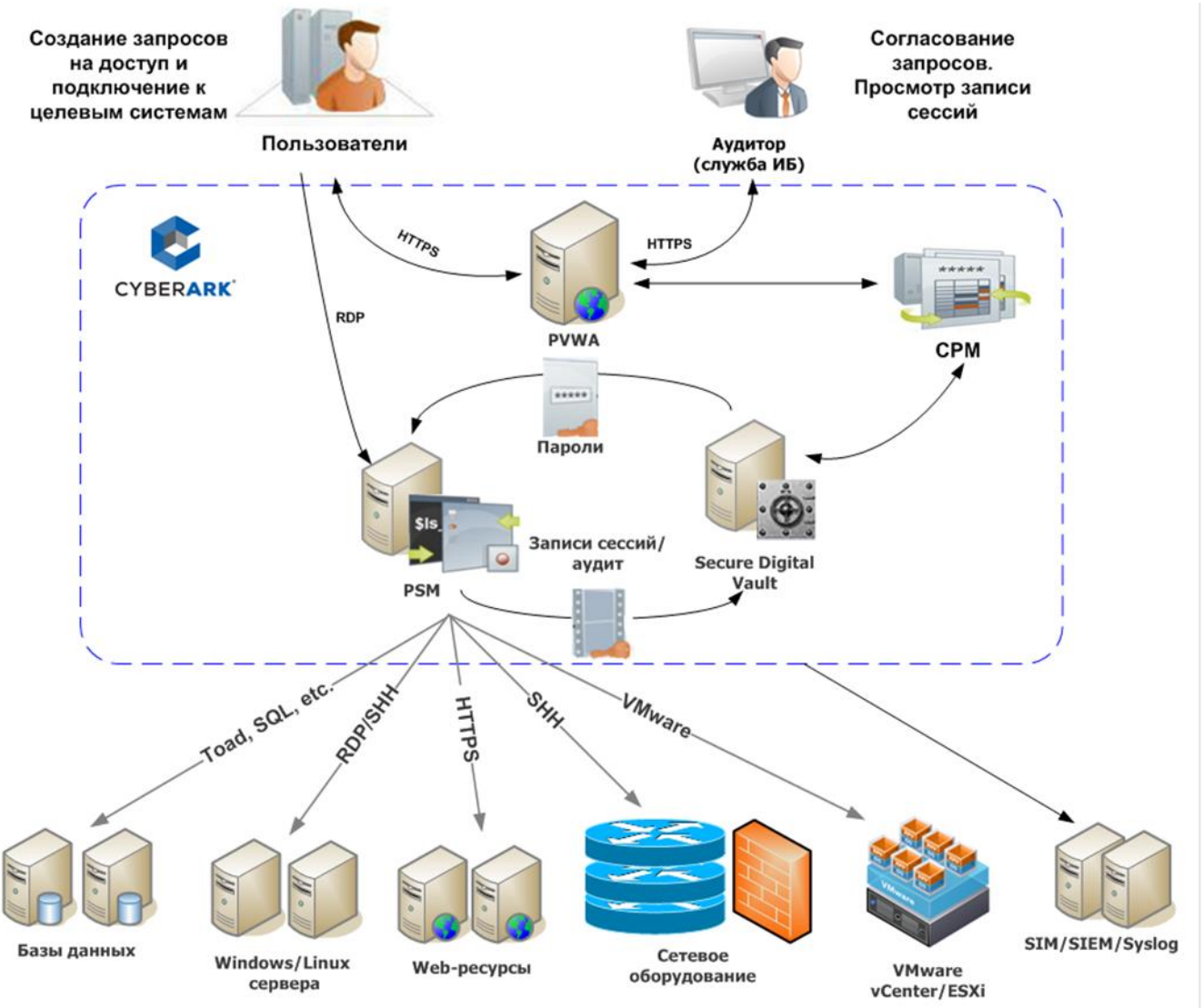

Рис.2.10. Етапи роботи з модулями Enterprise Password Vault і Privileged Session Manager

Таким чином Core Privileged Account Security, який являє собою повноцінне рішення для захисту, контролю та моніторингу привілейованих облікових записів в локальних мережах підприємств, в хмарі і гібридних інфраструктурах. Рішення CyberArk дозволить компаніям ефективно управляти параметрами привілейованих облікових записів і прав доступу, проактивного моніторингу та контролю за діями під привілейованими обліковими записами, «розумної» ідентифікації підозрілої активності та швидкої відповіді на загрози. Тому надалі розробимо рекомендації щодо ефективного використання основних модулів при впровадження їх на підприємстві.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ РІШЕННЯ CYBERARK PRIVILEGED ACCOUNT SECURITY

3.1. Рекомендації щодо застосування основних функціональних можливостей Core Privileged Account Security

Комплексне рішення Core Privileged Account Security складається з декількох компонентів, як це було розглянуто раніше.

Організації стикаються з великою кількістю проблем, пов'язаних із захистом, контролем і моніторингом привілейованих облікових записів, включаючи наступні:

Управління параметрами облікових записів. Багато IT-підприємств використовують ручні процеси, пов'язані з ротацією і оновленням параметрів доступу привілейованих облікових записів, які не захищені від помилок, - це неефективно, затратно і ризиковано.

Відстеження дій, здійснюваних під привілейованими обліковими записами. Часто організації не можуть централізовано здійснювати моніторинг і контроль за сесіями під привілейованими обліковими записами, піддаючи бізнес інформаційним загрозам.

Моніторинг і аналіз загроз. У багатьох організаціях відсутні повноцінні інструменти аналізу загроз, і вони не можуть проактивно ідентифікувати підозрілі дії і відпрацьовувати інциденти, пов'язані з безпекою.

Контроль доступу суперкористувача. Організації часто зазнають труднощів з ефективним контролем і аудитом доступу суперкористувача до критичних для бізнесу системам, збільшуючи тим самим ризики і складності в роботі.

Захист контролерів доменів Windows. Зловмисники можуть експлуатувати уразливості в протоколах аутентифікації Kerberos для того, щоб видавати себе за іншу особу для доступу до критичних IT-ресурсів і конфіденційної інформації.

В якості вирішення пропонується продукт Core Privileged Account Security, який являє собою повноцінне рішення для захисту, контролю та моніторингу привілейованих облікових записів в локальних мережах підприємств, в хмарі і гібридних інфраструктурах.

Надаймо загальні рекомендації щодо використання Core Privileged Account Security методами, за допомогою яких реалізується функціональність:

Централізований захист і контроль доступу для привілейованих облікових записів на основі певних адміністратором політик безпеки. Автоматична ротація паролів і SSH-ключів для привілейованих облікових записів вирішує проблему процесів, що здійснюються вручну, скорочується час обслуговування, а також виконується захист від випадкових помилок для адміністративних завдань, захисту облікових записів, що використовуються в локальних мережах, гібридних і хмарних середовищах.

Ізоляція і захист сесій привілейованих користувачів, а також захист цільових систем від шкідливих програм на кінцевих точках. Можливість моніторингу та запису дозволяє службам безпеки переглядати привілейовані сесії в реальному часі, автоматично припиняти або припиняти підозрілі сесії, а також здійснювати всебічний аудит дій привілейованих користувачів з підтримкою пошуку.

Визначення, сигналізування та протидія аномальній активності привілейованих користувачів. Це рішення збирає дані з багатьох джерел і застосовує складну комбінацію статистичних та детермінованих алгоритмів для визначення шкідливих дій під привілейованими обліковими записами.

*Контроль достатності прав доступу для * NIX і Windows.* Дане рішення дозволяє привілейованим користувачам запускати авторизовані адміністративні команди зі звичайних сесій в Unix або Linux без необхідності отримувати root-права. Це також дозволяє організаціям блокувати і стримувати атаки на Windows-сервера для зниження ризику крадіжки інформації або її шифрування з метою шантажу.

Захист контролерів доменів Windows. Дане рішення змушує використовувати мінімально необхідні права і контроль додатків на контролерах доменів, а також визначення атак на льоту. Це дозволяє протидіяти використанню чужих параметрів доступу і несанкціонованого доступу, а також допомагає захищатися від безлічі звичайних технік атак на Kerberos, включаючи Golden Ticket, Overpass-the-Hash та Privilege Attribute Certificate (PAC).

Такі функціональні можливості надають особливі переваги при використанні Core Privileged Account Security, а саме:

Зниження ризиків безпеки. Посилення захисту привілейованих облікових записів. Захист доступу до паролів і SSH-ключів привілейованих облікових записів. Ефективне визначення та протидію підозрілим і шкідливим діям. Захист від несанкціонованого доступу до привілейованих облікових записів, шахрайства та крадіжок інформації.

Зниження вартості і складності операцій. Усунення ручної роботи, зниження необхідного часу, а також недопущення випадкових помилок в процеси адміністрування. Спрощення операцій та збільшення ефективності роботи відділів, пов'язаних із забезпеченням інформаційної безпеки. Звільнення цінних IT-кадрів для концентрації уваги на стратегічні завдання на підтримку основних бізнес-активностей.

Допомога в задоволенні вимог законодавства. Установка заснованого на політиках контролю доступу привілейованих облікових записів для впевненості в задоволенні вимог регуляторів. Проста демонстрація політик і процесів аудиторам. Створення деталізованих аудиторських слідів і історії доступу для демонстрації задоволення вимог.

Швидка окупність. Захист і розширення попередніх інвестицій. Наявність інтеграції з коробки з широким списком IT-операцій і систем безпеки, включаючи системи аутентифікації, квиткових рішень, платформи особистого доступу і управління, а також з SIEM-рішеннями.

Покращення видимості. Розуміння того, які привілейовані облікові записи існують і у кого є до них доступ. Встановлення добре зрозумілих політик безпеки привілейованих облікових записів. Моніторинг дій під привілейованими обліковими записами в реальному часі і в ретроспективі.

3.2. Рекомендації щодо захисту привілейованих облікових записів за допомогою Enterprise Password Vault

Даний компонент забезпечує захист системи підприємств від атак, які використовують компрометацію привілейованих облікових записів, роботу якого показано на рис 3.1.

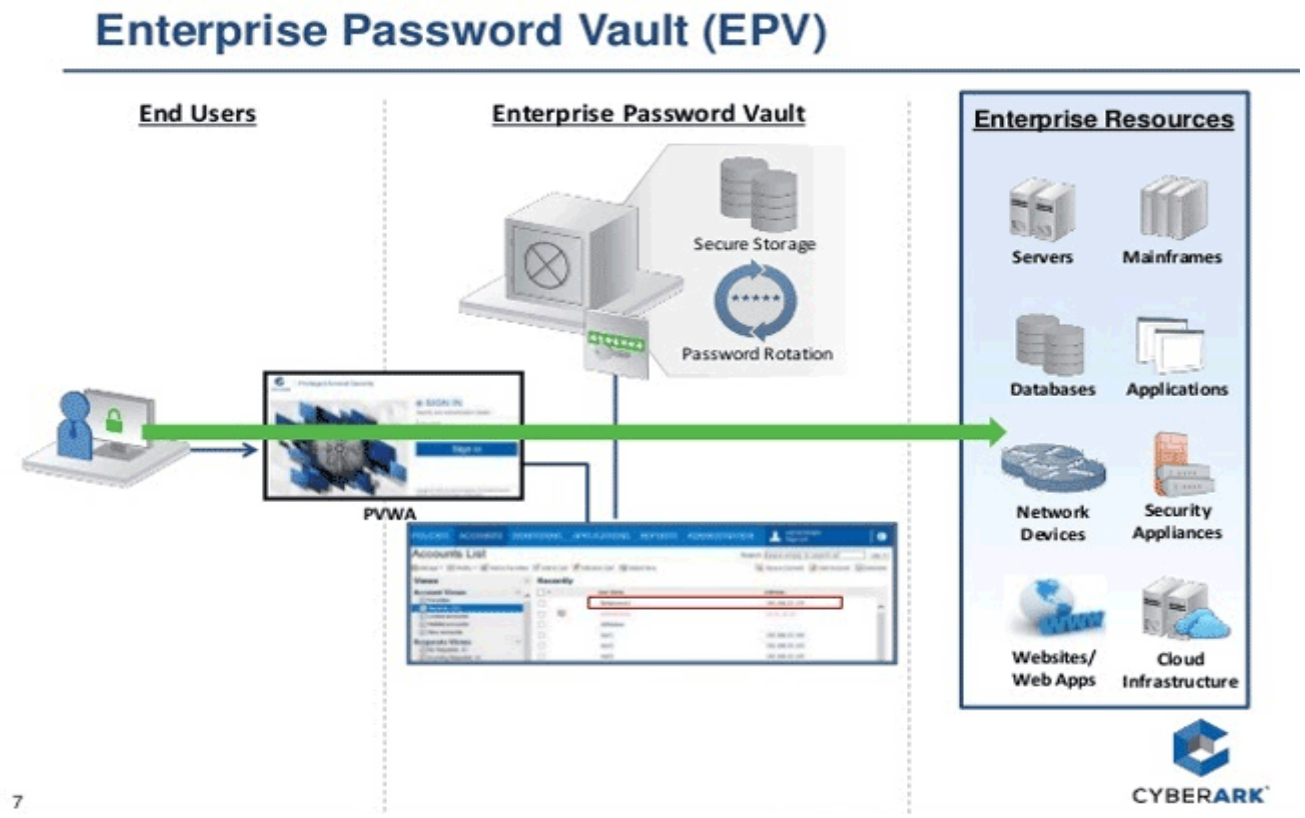

Рис.3.1. Схема роботи CyberArk Enterprise Password Vault

Надамо основні рекомендації, які необхідно розуміти при функціонуванні Enterprise Password Vault.

Гранульований контроль доступу привілейованих користувачів служить для запобігання доступу неавторизованих користувачів до параметрів привілейованих облікових записів. Тим самим гарантується, що авторизовані користувачі мають необхідний доступ, але необхідний тільки для легальних бізнес-цілей.

Реалізувати централізоване захищене сховище. Проводиться захист параметрів привілейованих облікових записів в локальних мережах, гібридних і хмарних середовищах, а також в межах груп, що працюють на принципі DevOps.

Використовується деталізований аудит і звітність. Співробітникам, які займаються безпекою і аудитом, надається прозоре бачення того, до чого має доступ кожен користувач з привілейованими і розподіленими обліковими записами, коли і чому.

Використовувати автоматичну ротацію параметрів доступу. Працює оновлення і синхронізація паролів і SSH-ключів привілейованих облікових записів через регулярні проміжки часу або за запитом, заснована на політиці.

Використовувати наскрізну автоматизацію. Дозволяє користувачам автоматизувати і спростити завдання, пов'язані з управлінням привілейованими обліковими записами за допомогою REST API, такі як обслуговування облікових записів, адаптація прав, видача дозволів та інше.

До основних переваг використання Enterprise Password Vault відноситься:

Для відділів, пов'язаних із забезпеченням безпеки, необхідно використати захист всіх паролів і SSH-ключів привілейованих облікових записів в захищеному центральному репозиторії для запобігання їх втрати, викрадення або несанкціонованого поширення.

Для спрощення управління правами через всебічний автоматизований контроль необхідно використовувати підхід "безпека понад усе»

Для спрощення проходження аудитів використовувати заснований на ролях контроль доступу, що вимагає від користувачів підтвердження прав. Також генерується повна і деталізована звітність і аудиторський слід для демонстрації відповідності вимогам.

3.3. Рекомендації використання контролю привілейованого доступу за допомогою Privileged Session Manager

У сучасних середовищах для спільної роботи організації повинні підтримувати ряд привілейованих облікових записів для доступу різних користувачів, включаючи сторонніх вендорів, підрядників, тимчасових співробітників і так далі.

З метою зменшення зовнішніх і внутрішніх ризиків, організації необхідно управляти і відстежувати сесії від імені привілейованих облікових записів без впливу на роботу кінцевих користувачів.

CyberArk Privileged Session Manager вирішує завдання ізоляції, моніторингу і контролю за привілейованими доступом до цінних активів підприємств. Детальний моніторинг і запис, який реалізовано в CyberArk Privileged Session Manager, дозволяє організаціям ізолювати, відстежувати, записувати і контролювати привілейовані сесії на критичних системах, включаючи Unixі Windows-системи, бази даних та віртуальні машини. Це рішення працює як jump-сервер і єдина контрольна точка контролю доступу, яка захищає від попадання шкідливих програм на цільову систему і записує натискання клавіш і команди для постійного моніторингу. Отримані деталізовані записи сесій і файли звіту для аудиту використовуються для спрощення проходження аудиту і прискорення судових розслідувань.

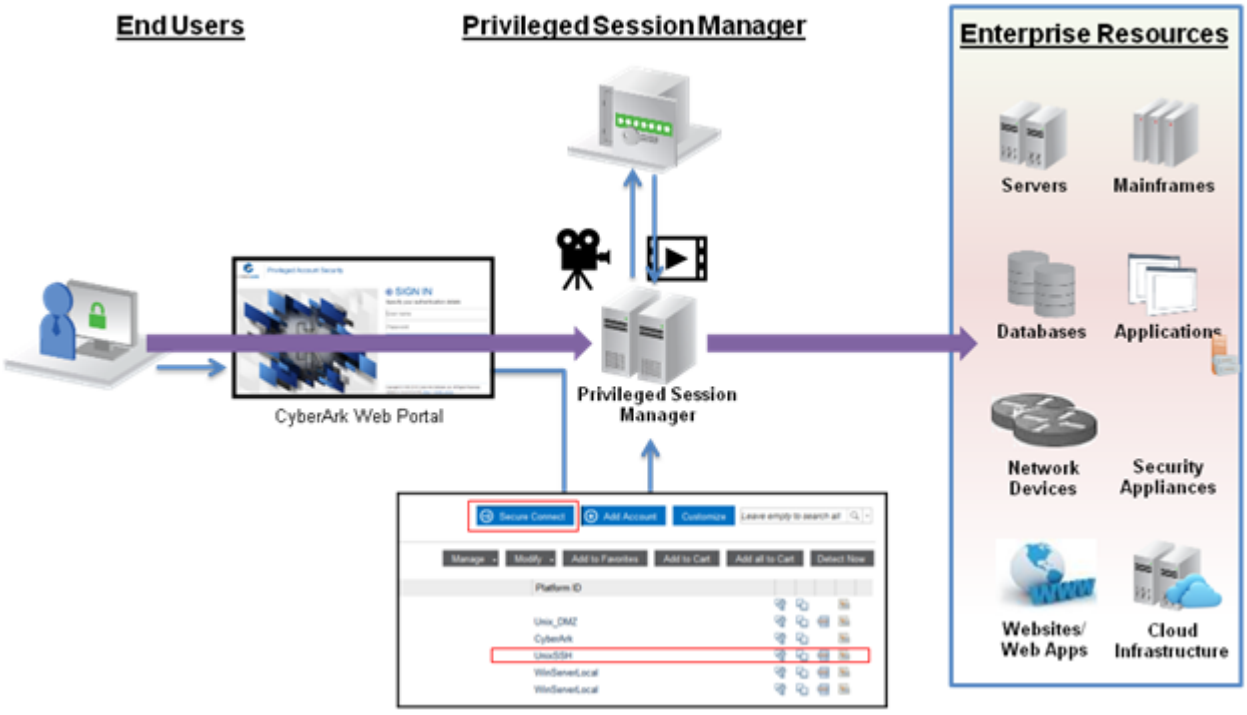

Рис.3.2. Схема роботи Privileged Session Manager

Privileged Session Manager - добре масштабується продукт, що підходить як невеликим підприємствам, так і великим. Privileged Session Manager - це безагентне рішення, розроблене для максимізації безпеки, включно із захищеними від підміни файли звітів для аудиту, примусовий моніторинг і запис, а також ізолювання сесій для захисту від поширення шкідливих програм. Універсальний конектор розширяє управління сесіями на всі компоненти IT-інфраструктури.

Рішення вбудовано в CyberArk Shared Technology Platform, та надає масштабованість, високу доступність, централізоване управління і звітність. Надамо основні рекомендації щодо використання функцій Privileged Session Manager:

Проводьте моніторинг в реальному часі, який дозволить фахівцям з інформаційної безпеки відслідковувати дії користувачів і визначати підозрілі події в реальному часі.

Застосовуйте віддалене припинення сесій, яке дозволяє фахівцям з інформаційної безпеки негайно завершувати підозрілі привілейовані сесії безпосередньо з консолі адміністратора CyberArk.

Переглядайте деталізовані файли звіту з підтримкою пошуку та відеозаписи дозволяють фахівцям з інформаційної безпеки точно визначати момент початку інциденту, розуміти, як почався інцидент, і швидко оцінити будь-які збитки.

Використана безагентна архітектура, яка заснована на проксі, надає єдину точку контролю доступу та здійснює примусовий моніторинг і запис всіх привілейованих дій.

Використовуйте захищений проксі-сервер. Захищений проксі-сервер створює ізольоване, захищене оточення шляхом відокремлення кінцевої машини користувача від цільової системи.

Використовуйте захищене цифрове сховище, яке зберігає записи сесій і файли звіту для перешкоджання від редагування користувачами історії їх дій.

Інтегруйте з додатковими рішеннями. Інтеграція з Enterprise Password Vault дозволяє приховати секрети (паролі / SSH ключі) привілейованого доступу від користувачів і гарантувати, що ці секрети ніколи не потраплять на їх робочі станції.

Інтеграція з Privileged Threat Analytics дозволяє організаціям автоматично аналізувати дії користувачів під час керованих привілейованих сесій і призначити рівні ризику актуальним і записаним сесій.

Таким чином, основні переваги, які надає Privileged Session Manager:

Дозволяє фахівцям з інформаційної безпеки визначати і припиняти атаку до того, як вона стане серйозною, за допомогою моніторингу та аналізу в реальному часі всіх дій в привілейованих сесіях.

Дозволяє фахівцям з інформаційної безпеки віддалено переривати підозрілі привілейовані сесії і потенційні атаки в їх процесі.

Прискорює час розслідування інцидентів і спрощує аудити за допомогою створення деталізованих файлів звітності з повною підтримкою пошуку і відеозаписів.

Інтеграція з Privileged Threat Analytics спрощує процес аудиту за допомогою можливості фахівців з IT-аудиту підвищувати або знижувати пріоритет перегляду сесії на основі рівня ризику.

Запобігання від обходу досвідченими користувачами моніторингу сесій і запобігання можливості відключенням.

Запобігає від приховування дій зловмисників за допомогою захищеного зберігання та контролю доступу до всіх файлів звітності і записів сесій.

Гарантує, що привілейовані паролі і SSH-ключі ніколи не потраплять до кінцевих користувачів або на їх робочі станції, запобігаючи будь неправильне використання або крадіжку параметрів привілейованого доступу.

Інтегрується з корпоративними платформами, як з коробки, так і за допомогою універсального конектора, надаючи широке покриття по оточенню і оптимальне впровадження.

Автоматизація та управління привілейованими завданнями підвищує продуктивність, покращує виробничі процеси і знижує ризики організацій по відношенню до критичних систем і додатків.

3.4. Рекомендації використання Privileged Threat Analytic для визначення і припинення атак в реальному часі

Даний компонент призначено визначати і припиняти атаки, що здійснюються в даний момент часу. У сучасних реаліях потрібно виходити з припущення, що атакуючі вже всередині інфраструктури. Вони часто залишаються нерозкритими, використовуючи доступ інших авторизованих користувачів. Цей внутрішній доступ дозволяє їм завдавати непоправної шкоди, яка призведе до погіршення репутації,

фінансових втрат і викрадення інтелектуальної власності. З цілеспрямованої аналітикою організації можуть визначати атакуючих швидше - навіть якщо вони виглядають як авторизовані користувачі, - даючи можливість фахівцям з інформаційної безпеки відповідати негайно і мінімізувати вікно можливостей для зловмисників (рис.3.3).

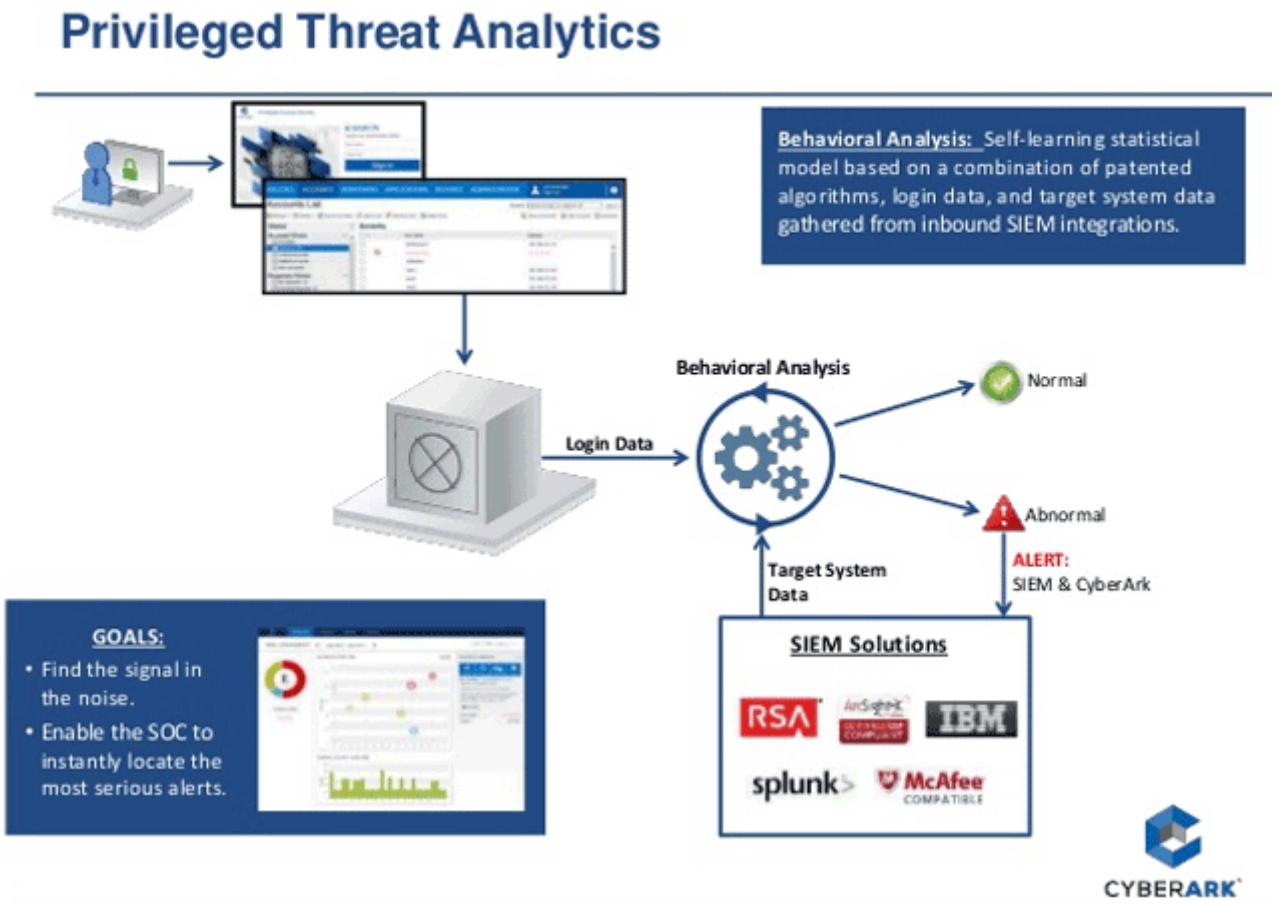

Рис.3.3. Схема роботи CyberArk Privileged Threat Analytics

CyberArk Privileged Threat Analytics, компонент рішення CyberArk Privileged Account Security - це розумна система безпеки, яка дозволяє організаціям визначати і реагувати на кібератаки, націлені на привілейовані облікові записи (Рис.3.4.). Це рішення розроблено для ідентифікації атак в реальному часі і автоматичної відповіді.

В основі рішення знаходиться аналітичний движок, діючий на складні комбінації закритих алгоритмів - включаючи детермінованіе і поведінкові - по

відношенню до користувачів, сутностей і мережевого трафіку для визначення індикаторів компрометації на ранньому етапі життєвого циклу атаки.

Визначаючи зловмисників раніше, фахівці з інформаційної безпеки отримують більше критично важливого часу, яке їм необхідно для можливості зупинити атаку перед тим, як вона зупинить бізнес.

Тому надамо основні рекомендації щодо використання функцій Privileged Threat Analytics, а саме:

Вбудовані пропрієтарні алгоритми керують привілейованими користувачами, сутностями і аналізують поведінку мережі для визначення раніше невизначених індикаторів атак, таких як підозра на викрадення параметрів доступу, приховані переміщення і ескалація привілеїв.

Самонавчальний аналітичний движок з часом звикає до облікового запису для визначення відхилень від авторизованих моделей поведінки.

Детектування атак на Kerberos дозволяє організаціям визначати і протидіяти потенційно катастрофічним атакам, які експлуатують уразливості в протоколі аутентифікації Windows.

Індекси ризику призначаються кожному окремому інциденту з метою допомоги в призначенні пріоритетів інцидентів.

Таргіновані, обгрунтовані попередження, що включають деталізовану інформацію про інцидент, дозволяють відповідальним співробітникам негайно реагувати на підозрілі дії.

Автоматична протидію на певні загрози спрощує відповідні дії, дозволяючи фахівцям з інформаційної безпеки негайно змінити параметри доступу до привілейованих облікових записів без необхідності втручання людини.

Деталізована панель з інформацією надають візуальну інтерпретацію інцидентів і рівня загроз, дозволяючи відповідальним співробітникам швидко переглядати інциденти в ретроспективі і здійснювати при необхідності негайних дій.

Інтеграція з SIEM-рішеннями дозволяє фахівцям з інформаційної безпеки використовувати існуючі розгорнуті SIEM для збору даних для таргентованої аналітики і для відправки повідомлень для виставлення пріоритетів інцидентів, які зачіпають привілейовані облікові записи.

Інтеграція з Privileged Session Manager дозволяє фахівцям з інформаційної безпеки визначати в реальному часі, коли дії з високим ризиком відбуваються під час привілейованої сесії і переривати підозрілі активні сесії.

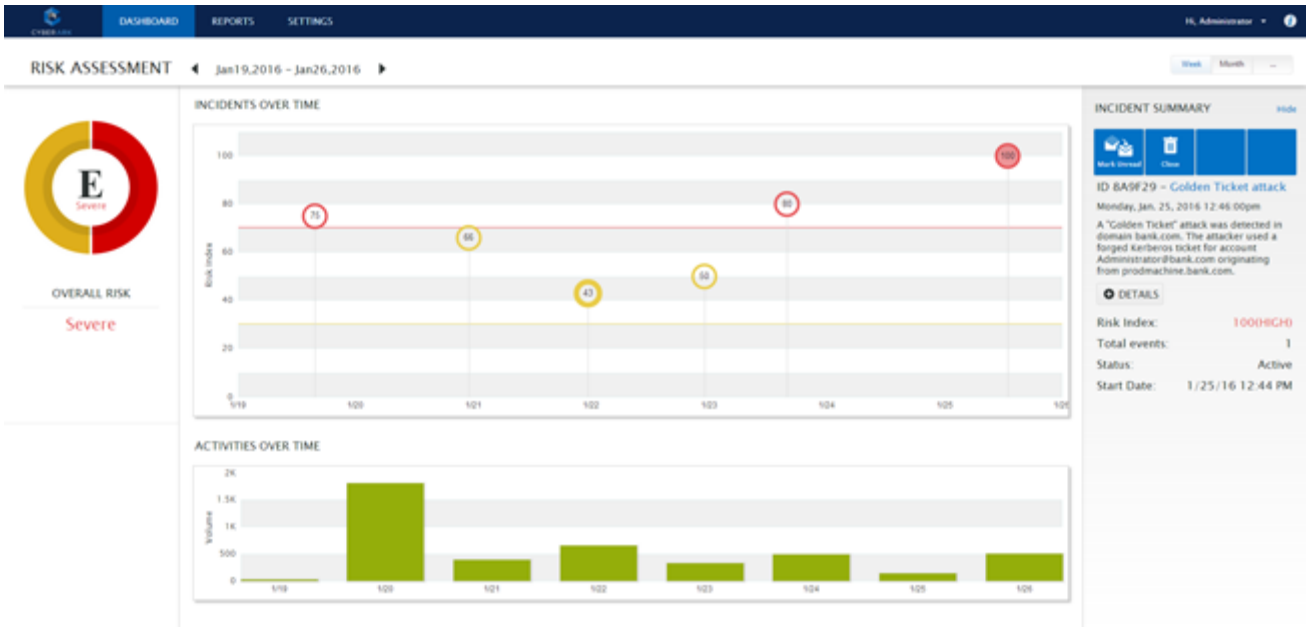

Рис 3.4. Веб-консоль CyberArk Privileged Threat Analytics

При використанні рекомендацій щодо використання функцій Privileged Threat Analytics можна отримати наступні переваги:

Кардинальне зменшення вікна можливості для зловмисників з місяців до секунд і скорочення збитків через швидке виявлення загроз на діях під привілейованими обліковими записами і критичних векторах атак.

Швидке визначення атак за допомогою аналітики, заснованої на вбудованих алгоритмах, написаних і постійно обновлюваних експертами в безпеки привілейованих облікових записів.

Адаптація визначення загроз для зміни ризикового оточення за допомогою алгоритмів машинного навчання, які постійно підлаштовуються під основну поведінку профілів, а також зміни авторизованої поведінки в часі.

Автоматична протидія при підозрі на крадіжку параметрів доступу до привілейованих облікових записів для зупинки зловмисника від продовження використання скомпрометованих параметрів доступу.

Прискорення розслідування інцидентів за рахунок надання деталізованої інформації по ним. Отримання швидкої окупності за допомогою використання існуючих агрегатів мережевих конекторів і конекторів на кінцевих точках з SIEM-рішень для безшовного колекціонування даних за допомогою існуючої інфраструктури.

Таким чином в даному розділі надано основні рекомендації щодо використання основних модулів Cyberark privileged account security та визначено їх переваги, що дозволить фахівцям з кібербезпеки підвищити ефективність функціонування корпоративної інформаційної системи.

ВИСНОВКИ

В результаті виконання магістерської роботи було отримано наступні результати:

Проведено аналіз вимог до користувачів корпоративної інформаційної системи, в результаті якого було визначено основні функції та призначення корпоративної інформаційної системи.

Для ефективного підтримання всіх бізнес процесів компанії було визначено, що необхідно проводити постійний контроль адміністраторів з супер правами з метою зменшення ризиків несанкціонованого доступу до корпоративної інформаційної системи.

Надалі було проведено аналіз методів та засобів управління привілейованими користувачами. На основі дослідження Gartner було визначено чинники, що впливають на зростання ринку щодо впровадження систем управління привілейованими користувачами PAM та обрано рішення CyberArk Privileged Access Security. Дане рішення може бути у вигляді програмного або хмарного використання.

В роботі було визначено життєвий цикл системи управління привілейованих користувачів. Постійне спостереження за використанням привілейованих облікових записів за допомогою аудитів та звітів допоможе виявити незвичайну поведінку, яка може вказувати на порушення або неправильне використання.

В роботі було визначено архітектуру та основні модулі Privileged Access Security.

На основі визначеної архітектури було розроблено рекомендації щодо комплексного використання модулів забезпечення безпеки привілейованого доступу.

Результати роботи доцільно використати для подальших досліджень та фахівцям кібербезпеки, які будуть впроваджувати дане рішення у своїх компаніях.

ПЕРЛІК ПОСИЛАНЬ

1. Герард Блокдик Полное руководство по управлению привилегированным доступом. – 2020. - 450с.

2. NIST Cybersecurity Framework.

3. Cyberark. Програма привілейованого доступу. [Електронний ресурс]. – Режим доступу: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/IMP-Program/IMP-Program-discoveryANDplanning.htm?tocpath=Get%20Started%7CImplementation%20Program%7C_____1.

4. Blueprint-for-PAM. [Електронний ресурс]. – Режим доступу: http://www.robyhill.com/yahoo_site_admin/assets/docs/Blueprint-for-PAM-Success-WP-1.8341041.pdf.

5. Архітектура PAM. [Електронний ресурс]. – Режим доступу: https://blog.51sec.org/2019/07/cyberark-notes.html.

6. Ядро привілейованого доступу. [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/practice/methods/core-privileged-account-security-cyberark

7. Peter Cheverton Key Account Management: Tools and Techniques for Achieving Profitable Key Supplier Status. - Kogan Page. – 2018. – 400p.

8. Larry Chambers Ken Ziesenheim Peter Trevisani Separate Account Management. – 2019.- 272p.

9. Мори Дж. Хабер Привилегированные векторы атак: создание эффективных стратегий киберзащиты для защиты организаций. – 2020. - 358с.

ДЕМОНСТРАЦІЙН МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)