ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ДАННИХ В КОРПОРАТИВНОМУ СЕРОДОВИЩІ ЗАСОБАМИ IBM GUARDIUM»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Охріменко С.В.
(прізвище та ініціали)
Керівник Дмітрієв В. Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Охріменко Сергію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія управління захистом кінцевих точок корпоративної інформаційної системи на платформі IBM Guardium»

керівник магістерської роботи Дмітрієв В'ячеслав Сергійович.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «13» жовтня 2020 року № 230.

2. Строк подання студентом магістерської роботи 15.12.2020 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси управління захистом корпоративної інформаційної системи;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту корпоративних інформаційних систем.
2. Склад та умови функціонування корпоративної інформаційної системи.
3. Методи та засоби управління захистом корпоративної інформаційної системи.
4. Варіант технології управління захистом корпоративної інформаційної системи.

5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об'єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу складу та умов функціонування корпоративної інформаційної системи.
4. Результати аналізу методів та засобів захисту корпоративної інформаційної системи.
5. Призначення, можливості та функції платформи IBM Guardium.
6. Архітектура та компоненти платформи IBM Guardium.

7. Додатки платформи IBM Guardium.

8. Варіант технології управління захистом корпоративної інформаційної системи.

9. Рекомендації щодо застосування технології управління захистом корпоративної інформаційної системи.

10. Висновки за результатами роботи.

6. Дата видачі завдання 01.10.2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту корпоративних інформаційних систем.	09.10.2020 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	30.10.2020 р.	
3.	Аналіз методів та засобів захисту корпоративної інформаційної системи.	16.11.2020 р.	
4.	Розроблення варіанту технології управління захистом корпоративної інформаційної системи.	23.11.2020 р.	
5.	Розроблення рекомендацій щодо застосування технології управління захистом корпоративної інформаційної системи.	02.12.2020 р.	
6.	Оформлення результатів дослідження.	09.12.2020 р.	
7.	Підготовка доповіді до захисту.	15.12.2020 р.	

Студент _____ Охріменко С.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи _____ Дмітрієв В. Є.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Охрісенко Сергія Володимировича
на тему: «Технологія захисту даних в корпоративному середовищі засобами IBM Guardium»

Актуальність:
Сьогодні захист периметра корпоративної інформаційної системи не є єдиним підходом забезпечення її кібербезпеки. Ландшафт сучасних загроз вимагає приділяти належну увагу захисту кожного джерела даних корпоративної інформаційної системи, а також комп'ютерів звичайних користувачів. Рішення для захисту потоків даних є найважливішим компонентом в будь-якій інформаційній системі і мережі, будучи засобом для захисту від атак ззовні через точку, яка захищається. Також ці рішення мають за мету забезпечення можливості контролю стану системи і обмеження певного функціоналу для її користувачів задля забезпечення кібербезпеки корпоративної системи в цілому. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми забезпечення захисту корпоративної інформаційної системи від новітніх загроз, визначено мета та завдання управління захистом корпоративної інформаційної системи.
2. Було досліджено методи та засоби управління захистом корпоративної інформаційної системи на платформі IBM Guardium.
3. Запропоновано варіант технології управління захистом корпоративної інформаційної системи на платформі IBM Guardium та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:
1. У магістерській роботі бажано було б провести саме порівняльний аналіз рішень корпоративної інформаційної системи різних виробників.
2. Запропонований варіант технології управління захистом кінцевих точок корпоративної інформаційної системи на платформі IBM Guardium бажано було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **задовільно**, а студент **Охріменко С. В.** – присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

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

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Охріменко С.В. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту даних в корпоративному середовищі засобами IBM Guardium».

Магістерська робота і рецензія додаються.

Директор інституту Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Охріменко С.В. за період навчання в інституті
(прізвище та ініціали студента)

ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) Черниш О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Охріменко С.В.*** обрав тему роботи, метою якої було дослідити зміст технології управління захисту корпоративної інформаційної системи на платформі IBM Guardium та розробити варіант технології управління ї] захистом на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Охріменко С.В. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Охріменко Сергія Володимировича на оцінку **«задовільно»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Керівник магістерської роботи Дмітрієв В. Є.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Охріменко С.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

РЕФЕРАТ

Текстова частина магістерської роботи: 70 сторінки, 9 рисунків, 19 джерел.

Об'єкт дослідження – процес забезпечення захисту даних в корпоративній інформаційної системи.

Предмет дослідження – технологія організації захисту корпоративної інформаційної системи.

Мета роботи – розробити варіант управління захистом корпоративної інформаційної системи та рекомендації щодо застосування технології захисту на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом корпоративної інформаційної системи.

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено мета та завдання управління захистом корпоративної інформаційної системи. Проведено аналіз існуючих технологій управління захистом корпоративної інформаційної системи.

Досліджено методи та засоби управління захистом корпоративної мережі на базі IBM GUARDIUM Визначено призначення, основні функції та склад платформи IBM GUARDIUM.

На основі досліджень проведених в роботі розроблено варіант технології управління захистом корпоративної інформаційної системи та рекомендації щодо застосування технології управління захистом на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ЗАХИСТОМ КОРПОРАТИВНОГО СЕРЕДОВИЩА, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ЗАХИСТОМ КОРПОРАТИВНОГО СЕРЕДОВИЩА, ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КОРПОРАТИВНОГО СЕРЕДОВИЩА

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС – корпоративна інформаційна система

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ШІ – штучний інтелект

AMP – Advanced Malware Protection

APT – Advanced Persistent Threats

BYOD – Bring Your Own Device

CRM – Customer Relationship Management

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

EMS – Endpoint Management System

ERP – Enterprise Resource Planning

EPP – Endpoint Protection Platform

IoC – Indicator of Compromise

IPS – Intrusion Prevention System

HIPS – Host-Based Intrusion Prevention System

MDM – Mobile Device Management

MDR – Managed Detection and Response

ML – Machine Learning

RBAC – Role-Based Access Control

SOC – Security Operations Center

UEBA – User And Entity Behavior Analytics

UEM – Unified Endpoint Management

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. Забезпечення безпеки корпоративного середовища в умовах кібернетичних впливів відноситься до методології захисту корпоративної мережі під час доступу через віддалені пристрої, такі як ноутбуки або інші бездротові і мобільні пристрої. Кожен пристрій з віддаленим підключенням до мережі створює потенційну точку входу для загроз безпеки.

Зазвичай безпека корпоративного середовища забезпечується системою, яка складається з програмного забезпечення безпеки, розташованого на центрально керованому і доступному сервері або шлюзі в мережі.. Сервер автентифікує логіни з кінцевих точок, а також оновлює програмне забезпечення пристрою при необхідності. Хоча програмне забезпечення для забезпечення безпеки корпоративного середовища розрізняється залежно від постачальника, можна очікувати, що більшість пропозицій програмного забезпечення будуть містити антивірусне та анти шпигунське програмне забезпечення, між мережевий екран, а також систему запобігання вторгнень.

Безпека корпоративного середовища стає все більш поширеною функцією кібербезпеки, оскільки обьем інформації, що циркулює у корпоративній інформаційній системі збільшується кожного дня за рахунок інформаційного періоду розвитку суспільства.

Це визначає актуальність дослідження щодо організації активного захисту корпоративної інформаційної системи на базі IBM GUARDIUM.

Об'єкт дослідження – процес забезпечення захисту даних в корпоративній інформаційної системи.

Предмет дослідження – технологія організації захисту корпоративної інформаційної системи.

Мета роботи – розробити варіант управління захистом корпоративної інформаційної системи та рекомендації щодо застосування технології захисту на підприємстві.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту корпоративної інформаційної системи;

встановити сутність завдань управління захистом корпоративної інформаційної системи;

проаналізувати існуючі технології управління захистом корпоративної інформаційної системи;

проаналізувати методи та засоби управління захистом корпоративної інформаційної системи;

проаналізувати основні функції та принципи реалізації управління захистом корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом корпоративної інформаційної системи.

Практичне значення одержаних результатів полягає в розробці варіанта технології управління захистом корпоративної інформаційної системи на базі IBM GUARDIUM., а також у розробці рекомендацій щодо застосування технології управління захистом корпоративної інформаційної системи.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Під інформаційною безпекою підприємства або компанії розуміють комплекс заходів організаційного та технічного характеру, направлених на збереження та захист інформації та її ключових елементів, а також обладнання та системи, які використовуються для роботи з інформацією, її зберігання та передачі. Цей комплекс включає технології, стандарти і методи управління інформацією, які забезпечують її ефективний захист [2].

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

Корпоративна інформаційна система (КІС) — це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві (в корпорації) і постачає інформацію для прийняття управлінських рішень. У ній реалізована управлінська ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології.

Сучасні КІС мають такі основні характеристики:

1. Масштабність

Це одна із важливих характеристик інформаційних систем такого класу, враховуючи масштаби діяльності корпорації. Масштабна ІС повинна функціонувати на масштабній програмно-апаратній платформі (сервери, операційні системи, системи комунікації, СУБД), що потребує значних зусиль спеціалістів з проектування й упровадження таких систем. Оскільки варіантів конфігурації базового устаткування і програмного забезпечення може бути багато, то КІС має бути багатоплатформною.

2. Багатоплатформні обчислення

В КІС виникає потреба, щоб прикладна програма працювала на кількох програмно-апаратних платформах. При цьому мають бути забезпечені однакові

інтерфейс і логіка роботи на всіх платформах, маючи на увазі подібність схем екрана, елементів меню та діалогової інформації, що надається користувачеві різними платформами; інтегрованість з користувацьким операційним середовищем; однакова поведінка на різних платформах; узгоджена підтримка незалежно від платформи тощо. Реалізувати прикладну програму одночасно в кількох середовищах нелегко. Тому з'явилися інтегровані програмні середовища розробки (Framework), які значно полегшують перенесення прикладних програм між різними середовищами. До них належать Windows Open Systems Architecture (WOSA); Win 32, загальне відкрите програмне середовище UNIX COSE, App Ware Foundation та інші.

3. Робота в неоднорідному обчислювальному середовищі

Важливою перевагою КІС є можливість роботи в мережах, до яких входять комп'ютери, що працюють під управлінням різних операційних систем або побудовані на різних обчислювальних платформах. При цьому має бути забезпечена взаємодія всіх робочих обчислювальних платформ і операційних систем, які використовуються.

4. Розподілені обчислення

Це один із видів роботи в клієнт-серверній архітектурі, коли дані чи запити, що надходять з клієнтських машин, розподіляються поміж кількома серверами, що збільшує пропускну здатність для користувача і дає можливість багатозадачної роботи. Це сприяє максимальному використанню обчислювальних ресурсів, зниженню витрат і підвищенню ефективності системи. Забезпечення розподіленої роботи і віддаленого доступу до документів — обов'язкова вимога до інформаційних систем корпоративного рівня. Останніми роками невід'ємною складовою частиною цієї вимоги стала підтримка роботи в архітектурі Internet/Intranet.

КІС надає користувачеві можливість вирішення таких глобальних задач:

1. Зробити прозорим для керівництва корпорацією використання вкладених у бізнес капіталів;

2. Надати повну інформацію для економічної доцільності стратегічного планування;

3. Професійно керувати витратами, наочно і своєчасно показувати, за рахунок чого можна мінімізувати витрати;

4. Реалізувати оперативне управління підприємством згідно з вибраними ключовими показниками (собівартість продукції, структура витрат, рівень прибутковості тощо);

5. Забезпечити гарантовану прибутковість підприємства за рахунок оптимізації і прискорення ряду процесів (строків виконання нових замовлень, перерозподілу ресурсів і т.д.).

Повноцінна КІС повинна забезпечити інформаційну прозорість підприємства, формувати єдиний Інформаційний простір, який об'єднує інформаційні потоки, що йдуть від виробництва до нього, з даними фінансово-господарських служб і видавати необхідні повідомлення для всіх рівнів управління підприємства.

Види корпоративних інформаційних систем

Корпоративні інформаційні системи поділяються на наступні класи:

1. ERP(Enterprise Resource Planning System)(Планування ресурсів підприємства)

Сучасні ERP з'явилися в результаті майже сорокалітньої еволюції управлінських та інформаційних технологій. Призначені вони головним чином для побудови єдиного інформаційного простору підприємства (об'єднання всіх відділів і функцій), ефективного управління всіма ресурсами компанії, пов'язаними з продажами, виробництвом, обліком замовлень. Будується ERP-система за модульним принципом і, як правило, має у своєму складі модуль безпеки для запобігання як внутрішніх, так і зовнішніх крадіжок інформації.

Проблеми ж виникають в основному через помилки використання або початкового плану впровадження системи. Наприклад, урізані інвестиції в навчання персоналу роботі в системі суттєво знижують ефективність. Тому впроваджують ERP-системи як правило не відразу в повному обсязі, а окремими модулями, особливо на початковій стадії.

Рис. 1.1. Функціональний склад ЕРП

2. CRM (Customer Relationship Management System)(Управління відносинами з клієнтами)

Управління відносинами з клієнтами— поняття що охоплює концепції, котрі використовуються компаніями для управління їхніми взаємовідносинами зі споживачами, включаючи збір, зберігання й аналіз інформації про споживачів, постачальників, партнерів та інформації про взаємовідносинами з ними. Сучасна CRM направлена на вивчення ринку і конкретних потреб клієнтів. На основі цих знань розробляються нові товари або послуги і таким способом компанія досягає поставлених цілей і покращує свій фінансовий показник.

Існує три CRM-підходи, кожний з котрих може бути реалізованим окремо від інших:

1. Оперативний— автоматизація споживчих бізнес-процесів, що допомагає персоналу з роботи з клієнтами виконувати свої функції.

2. Співробітницький— програма взаємодіє зі споживачами без участі персоналу з роботи з клієнтами.

3. Аналітичний— аналіз інформації про споживачів із різноманітними цілями.

Принципи CRM-систем:

1. Наявність єдиного сховища інформації, звідки в будь-який момент доступні усі відомості про усі випадки взаємодії з клієнтом;

2. Синхронізація управління множинними каналами взаємодії;

3. Постійний аналіз зібраної інформації про клієнтів та прийняття відповідних організаційних рішень— наприклад, «сортування» клієнтів на основі їхньої значимості для компанії.

Можливості CRM-систем:

- Швидкий доступ до актуальної інформації про клієнтів;
- Оперативність обслуговування клієнтів та проведення операцій;
- Формалізація схем взаємодії з клієнтами, автоматизація документообігу;
- Швидке отримання всіх необхідних звітних даних та аналітичної інформації;
- Зниження операційних витрат менеджерів;
- Контроль роботи менеджерів;
- Узгоджена взаємодія між співробітниками і підрозділами.
- Управління бізнес-процесами — дозволяє автоматизувати послідовні операції, які виконуються співробітниками організації;
- Управління контактами, історія взаємодії з клієнтами — це єдина база даних всіх контрагентів компанії (клієнтів, постачальників, конкурентів) з внесеною раніше докладною інформацією про них, про їх співробітників і т.д.

Система дозволяє здійснювати швидкий пошук важливої інформації про контрагентів, отримувати всю історію зустрічей, переговорів, листування, угод та інше. Це дуже зручний інструмент для швидкої і якісної роботи з величезними масивами інформації про клієнтів. Система автоматично нагадує про необхідність зробити дзвінок, про заплановані зустрічі та інші заходи;

CPM дозволяє складати плани за різними показниками (дохід з продажу по менеджерам, відділам, продуктам …). По історії проектів можна відбудувати воронку продажів, що дозволяє визначати проблемні зони в циклах продажів. Планування і контроль виконання плану по факту. Є можливість ведення різних прайс-листів (оптових, дрібнооптових, роздрібних), враховувати акційні пропозиції, знижки від обсягу покупки.

Вся робота з клієнтом відбувається в одній системі:

- Планування заходів, здійснення угод, підготовка і виписка необхідних звітних документів;
- Планування та управління закупівлями і доставками — в системі менеджери завжди можуть бачити наявність і кількість товарів на складі. Відповідальні співробітники можуть стежити за виконанням плану закупівель;
- Управління маркетингом — електронна розсилка, пряма розсилка, sms розсилання. Система дозволяє управляти маркетинговими заходами і визначати їхню результативність. Можливість сегментації наявних в базі клієнтів (діючих і потенційних) за певними параметрами для проведення маркетингових заходів;
- Автоматизація документообігу — в систему можна ввести шаблони будь-яких документів, які використовуються в організації, при цьому зникає необхідність ручного складання нового документа при виникненні події. Швидке автоматичне заповнення шаблонів договорів, які зберігаються в системі. Автоматичне виставлення рахунків і контроль оплати по них через сумісність з Клієнт-банком;
- Можливість роботи по мережі;
- Імпорт контрагентів з інших баз.

3. MES (Manufacturing Execution System)(Керування виробництвом)

Системи класу MES призначені для виробничого середовища підприємства. Системи цього класу відстежують і документують весь виробничий процес, відображають виробничий цикл в реальному часі. На відміну від ERP, яка не має безпосереднього впливу на процес, за допомогою MES стає можливим коригувати (або повністю перебудовувати) процес стільки разів, скільки це буде потрібно. Інакше кажучи, системи такого класу призначені для оптимізації виробництва і підвищення його рентабельності. Збираючи та аналізуючи дані, одержувані, наприклад, від технологічних ліній, вони дають більш детальне уявлення виробничої діяльності підприємства (від формування замовлення до відвантаження готової продукції), покращуючи фінансові показники підприємства. Всі головні показники, які входять в основний курс економіки

галузі (віддача основних фондів, обіг грошових коштів, собівартість, прибуток і продуктивність) детально відображуються в ході виробництва. Фахівці називають MES мостом між фінансовими операціями ERP-систем і оперативною діяльністю підприємства на рівні цеху, ділянки або лінії.

Рис. 1.2 Функціональний склад MES

4. WMS (Warehouse Management System)(Система Управління Складом)

Warehouse Management System — система управління, що забезпечує автоматизацію та оптимізацію всіх процесів складської роботи профільного підприємства.

Архітектура автоматизованої інформаційної системи управління складом

Архітектура автоматизованої інформаційної системи управління складом побудована за трирівневим принципом:

- перший компонент являє собою видиму для користувача частину — інтерфейс типу «людина-машина» — «клієнтський додаток», за допомогою якого користувач здійснює введення, зміну та видалення даних, дає запити на виконання операцій та запити на вибірку даних (одержання звітів);
- другий компонент (прихована від користувачів частина системи) — сервер бази даних, здійснює зберігання даних. Користувач через клієнтський додаток ініціює процедуру запиту на вибірку, введення, зміну або видалення даних у базі даних (БД);

- третій компонент — бізнес-логіка («завдання» або «процеси» — спеціалізовані програми обробки) здійснює ініційовану користувачем обробку даних, і повертає оброблені дані в БД, повідомляючи користувачеві через екран клієнтського додатку про завершення запитаної обробки.

Цілі впровадження:

- активне управління складом;
- збільшення швидкості набору товару;
- отримання точної інформації про місце знаходження товару на складі;
- ефективне управління товаром, що має обмежений термін придатності;
- отримання інструменту для підвищення ефективності і розвитку процесів по обробці товару на складі;
- оптимізація використання складських площ.

5. EAM (Enterprise Asset Management) (Система управління фондами підприємства)

Система управління основними фондами підприємства, що дозволяє скоротити простої устаткування, витрати на техобслуговування, ремонти і матеріально-технічне постачання. Являє собою необхідний інструмент в роботі фондомістких галузей (енергетичних, транспортних, ЖКГ, добувної промисловості і т.д.).

Основні фонди — це засоби праці, які багаторазово беруть участь у виробничому процесі, зберігаючи при цьому свою натуральну форму, поступово зношуючи, переносячи свою вартість по частинах на знов створювану продукцію. У бухгалтерському та податковому обліку, відображені в грошовому вираженні основні фонди називаються основними засобами. Історично EAM-системи виникли з CMMS-систем (ще одного класу ІС, управління ремонтами). Зараз модулі EAM входять також до складу великих пакетів ERP-систем (таких як mySAP Business Suite, IFS Applications, Oracle E-Business Suite та ін.)

6. HRM (Human Resource Management) (Система управління персоналом)

Система управління персоналом — є однією з найважливіших складових частин сучасного менеджменту. Основна мета таких систем — залучення та

утримання цінних для підприємства кадрових фахівців. HRM-системи вирішують два головні завдання: упорядкування всіх облікових і розрахункових процесів, пов'язаних з персоналом, і зниження відсотка відходу співробітників. Таким чином, HRM-системи в певному сенсі можна назвати «CRM-системами навпаки», залучати та утримувати не покупців, а власних співробітників компаній. Зрозуміло, методи тут застосовуються зовсім інші, але загальні підходи схожі. Функції HRM-систем:

- Пошук персоналу;
- Підбір та відбір персоналу;
- Оцінка персоналу;
- Навчання та розвиток персоналу;
- Управління корпоративною культурою;
- Мотивація персоналу;
- Організація праці. [1]

1.2. Аналіз проблеми забезпечення захисту інформації корпоративного середовища

Під інформаційною безпекою підприємства або компанії розуміють комплекс заходів організаційного та технічного характеру, спрямованих на збереження та захист інформації та її ключових елементів, а також обладнання та системи, що використовуються для роботи з інформацією, її зберігання та передачі. Цей комплекс включає технології, стандарти та методи управління інформацією, які забезпечують її ефективний захист.

Забезпечення інформаційної безпеки допомагає захистити інформацію та інформаційну інфраструктуру підприємства від негативних впливів. Такі дії можуть мати випадковий або навмисний, внутрішній або зовнішній характер.

Результатом таких втручань може стати втрата важливої інформації, її несанкціонована зміна чи використання третіми особами. Тому інформаційна

безпека – це важливий аспект захисту бізнесу та забезпечення його безперервності.

Принципи ефективного впровадження у компанії систем інформаційної безпеки:

1. Конфіденційність.

Під конфіденційністю розуміють організацію та підтримку ефективного контролю для забезпечення достатнього ступеня безпеки даних, активів та інформації на різних етапах бізнес-процесів для виключення несанкціонованого чи небажаного розкриття. Підтримка конфіденційності обов'язково застосовується при збереженні та транзиті інформації у будь-якому форматі.

2. Цілісність.

Цілісність охоплює елементи управління, які забезпечують внутрішню та зовнішню послідовність інформації. Забезпечення цілісності дає змогу виключити можливість спотворення даних на будь-якому з етапів ділових операцій.

3. Доступність.

Доступність підтримує повноцінний та надійний доступ до інформації для посадових осіб, які мають відповідні повноваження. Ключовим моментом тут є передбачуваність процесів, що протікають у мережному середовищі, щоб користувачі мали можливість доступу до необхідних даних у потрібний час. Одним із важливих факторів доступності інформації є можливість швидкого та повного відновлення системи після збоїв, щоб не допустити його негативного впливу на функціонування компанії.

Здійснення контролю інформаційної безпеки підприємства

Забезпечити повноцінну та надійну інформаційну безпеку підприємства можна лише за умови застосування комплексного та системного підходу. Система інфобезпеки має бути побудована з урахуванням усіх актуальних загроз та вразливостей, а також з урахуванням тих загроз, які можуть виникнути в майбутньому. Тому важливо забезпечити підтримку безперервного контролю, який має діяти щодня та цілодобово. Необхідною умовою є забезпечення контролю на кожному з етапів життєвого циклу інформації, починаючи з моменту

її надходження до інфраструктури компанії і закінчуючи втратою її актуальності чи знищенням даних.

Існує кілька видів контролю інформаційної безпеки, впровадження яких дозволяє компанії знижувати ризики у цій сфері та підтримувати їх на прийнятному рівні. У тому числі розрізняють:

• Адміністративний контроль.

Адміністративний контроль інформаційної безпеки - це система, що складається з комплексу встановлених стандартів, принципів та процедур. Цей вид контролю визначає межі для здійснення бізнес-процесів та управління персоналом. Він включає законодавчі та нормативні акти, прийняту на підприємстві політику корпоративної безпеки, систему найму працівників, дисциплінарні та інші заходи.

• Логічний контроль.

Логічний контроль передбачає використання засобів управління (засобів технічного контролю), що захищають інформаційні системи від небажаного доступу. Ці засоби об'єднують спеціальне ПЗ, брандмауери, паролі тощо.

• Фізичний контроль.

Фізичний контроль зосереджений серед робочих місць і засобів обчислення. У тому числі він передбачає забезпечення ефективного функціонування інженерних систем будівель підприємства, робота яких може вплинути на зберігання та передачу інформації. До таких систем відносяться опалення та кондиціювання, протипожежні системи. Іншою важливою складовою фізичного контролю є системи контролю та управління доступом на об'єкти. [2]

1.3. Мета та завдання захисту інформації у корпоративному середовищі

Оскільки корпоративним середовищем можна вважати будь яку структурну організацію, очевидно, що така система захисту може буди використана у будь якій не спеціалізованій інформаційній системі, тобто не у банках/державних установах/КВОІ, а у кожній приватній організації, організаціях, що не

використовують конфіденційну інформацію, що відноситься до власності держави, та не є фінансовою організацією

У зв’язку з таким широким спектром використання необхідно організувати захист інформації, що циркулює в автоматизованій системі з метою збереження її цілісності доступності та конфіденційності, що дозволить зберегти репутацію компанії, не допустити створення монополій в результати зловмисних дій конкурентів, захистити права і свободи як співробітників, так і клієнтів організації у відповідності до нормативної документації Держави, починаючи з конституції, так закінчуючи галузевими стандартами.

1.4. Аналіз існуючих технологій захисту інформації у корпоративному середовищі

Війну між захисниками даних і злодіями даних описують як гру у «кішки-мишки». Як тільки білі капелюхи протистоять одній формі зловмисної поведінки чорного капелюха, інша злісна форма піднімає свою потворну голову. Як можна схилити ігрове поле на користь воїнів інформаційної безпеки Ось п’ять нових технологій безпеки, які можуть бути в змозі зробити це.

1. Апаратна автентифікація

Недостатність імен користувачів і паролів добре відома. Очевидно, потрібна форма автентифікації. Один із способів — запустити автентифікацію в користувача обладнання. Intel рухається в цьому напрямку з рішенням Authenticate у своєму новому процесорі Core vPro шостого покоління. Він може поєднувати різноманітні апаратні засоби в той же час, щоб підтвердити ідентичність користувача. Intel спирається на попередні зусилля, щоб виділити частину чіпсета для безпеки функції, щоб зробити пристрій частиною процесу автентифікації. Гарна автентифікація вимагає від користувачів три речі: те, що вони знають, наприклад пароль; хто вони, наприклад ім'я користувача; і те, що вони мають, наприклад, жетон. У разі автентифікації, пристрій стає тим, що у вас є. «Це не нове», — сказав Скотт Кроуфорд, директор з досліджень інформаційної

безпеки. «Ми бачили це в інших проявах, таких як технології ліцензування та жетони». Апаратна автентифікація може бути особливо важливою для Інтернету речей (IoT), де мережа хоче переконатися, що річ, яка намагається отримати до неї доступ, повинні мати до нього доступ. Однак Кроуфорд зазначив: «Найбільш безпосереднє застосування цієї технології – це для автентифікації кінцевої точки в традиційному IT-середовищі — ноутбуках, настільних комп'ютерах і мобільних пристроях з використанням чіпсетів Intel».

2. Аналітика поведінки користувачів

Коли чиєсь ім'я користувача та пароль зламані, той, у кого вони є, увійти в мережу та брати участь у всіх видах шкідливої поведінки. Така поведінка може спровокувати червоний прапорець для системних захисників, якщо вони використовують аналітику поведінки користувачів (UBA). Технологія використовує аналітику великих даних для виявлення аномальної поведінки користувача. «На підприємстві є великий інтерес до цього», — сказав Кроуфорд 451. «Активність користувачів є проблемою номер один для професіоналів у сфері безпеки». Він пояснив, що ця технологія усуває сліпу зону безпеки підприємства. «Коли зловмисник проникає на підприємство, що буде потім?» — запитав він. «Перше, що вони роблять, - це компроміс з обліковими даними. Тоді виникає питання: чи можна розрізняти активність законного користувача та зловмисника, який отримав доступ, скомпрометував облікові дані законного користувача і тепер шукає інші цілі?" Видимість діяльності, яка не відповідає нормі законного користувача, може закрити уразливість в середині ланцюга атаки. Порівняння теперішньої поведінки користувача з поведінкою в минулому – це не єдиний спосіб, яким це може зробити UBA, визначити зловмисника. «Є щось, що називається «рівний аналіз», — пояснив Стівен Гроссман, віце-президент з управління програмами Bay Dynamics, аналітика загроз компанії. «Це порівнює те, як хтось поводиться, порівняно з людьми з таким же керівником або того ж відділу. Це може бути показником того, що людина робить те, чого вони не повинні робити, або хтось інший заволодів їхнім обліковим записом». Крім того, UBA може бути цінним інструментом для навчання співробітників покращенню культури безпеки. «Одна з найбільших проблем компанії – це те, що

працівники не стежать за політикою безпеки компанії, — сказав Гроссман. — Щоб мати можливість ідентифікувати цих людей і пом’якшити їх ризик, який, пов’язаний з їх належним навчанням, є критичним». «Користувачів можна ідентифікувати та автоматично зареєструвати на тренінг, відповідний до політики, яку вони порушували».

3. Запобігання втрати даних

Ключем до запобігання втрати даних є такі технології, як шифрування та токенізація. Вони можуть захищати дані до фізичного рівня, що може принести користь підприємству.

«Не може бути надійного шифрування без керування ключами, і не може бути ключа керування без надійної автентифікації».

4. Глибоке навчання

Глибоке навчання охоплює ряд технологій, таких як штучний інтелект і машинне навчання. «Незалежно від того, як це називається, є великий інтерес до нього в цілях безпеки", - сказав Кроуфорд з 451. Як і аналітика поведінки користувачів, глибоке навчання фокусується на аномальній поведінці. "Ти хочеш зрозуміти, де шкідлива поведінка відхиляється від законної чи прийнятної поведінки з точки зору безпеки», – пояснив Кроуфорд. «Коли ви дивитеся на активність у корпоративній мережі, є поведінка, якої не має поведінка користувача, але все ще є шкідливою. Замість того, щоб дивитися на користувачів, система дивиться на "об'єкти", пояснив Бред Медейрі, старший віце-президент Буз Аллена. «Точна бізнес-аналітика та останні відкриття в моделях машинного навчання означають, що тепер ми можемо дивитися на різних суб'єктів, які існують на рівні підприємства на мікро- та макрорівнях. Наприклад, а ЦОД, як сутність, може вести себе певним чином, подібно до користувача». «Використання машинного навчання може допомогти подолати прокляття розширених постійних загроз», - додав Кріс Лавджой, президент компанії Acuity Solutions, виробника передового програмного забезпечення з виявлення шкідливої поведінки. «З його здатністю обирати між «хорошим» і «поганим» програмним забезпеченням важлива швидкість, технології машинного навчання запропонують значну користь для організації безпеки, які прагнуть скоротити час на розширене

виявлення та ліквідацію загроз», - вона сказала. Кроуфорд сказав, що очікує інвестицій у глибоке навчання з метою продовжити дослідження у напрямку організації захисту. Однак він додав, що «завдання для підприємств у тому, що їх багато компанії, що виходять на ринок з подібними підходами до тієї ж проблеми. Розмежування відмінностей від одного постачальника до іншого буде серйозною проблемою для підприємств у наступному році та далі».

5. Хмара

«Хмара матиме трансформаційний вплив на індустрію технологій безпеки загалом", - сказав Кроуфорд.. Локальні методи будуть перенесені в хмару. Речі такі як віртуалізоване обладнання безпеки, віртуалізовані брандмауери та віртуалізоване вторгнення системи виявлення та запобігання. Але це буде проміжний етап. «Якщо ви думаєте про те, що може зробити постачальник інфраструктури як послуги на дуже великому рівні масштабу для всіх своїх клієнтів, може не виникнути потреби вилучати всі засоби захисту, — сказав Кроуфорд. — Постачальник інфраструктури як послуги створить це на їхню платформу, що позбавить від необхідності робити це для окремої хмари клієнта». Пескатор додав, що державні установи та приватна промисловість збільшили безпеку своїх центрів обробки даних за допомогою послуг IaaS, таких як Amazon і Firehost. «Програма GSA FedRAMP — чудовий приклад «сертифікованої достатньо безпечної» хмарної послуги», - сказав він [15].

Gartner’s топ 10

Як групи інформаційної безпеки забезпечують найефективнішу підтримку бізнесу та ризики управління.

Сучасні команди з інформаційної безпеки стикаються з проблемами, унікальними для поточного бізнесу в навколишньому середовищі. Хоча головною метою команди є підтримка цифрового бізнесу, що розвивається, вони також мають справу зі все більш розвиненим середовищем загроз. Біля Gartner Security & Risk Management Summit, Ніл Макдональд, віце-президент Gartner, розповів про останні технологічні тенденції 2016 року, які дозволяють командам інформаційної

безпеки забезпечувати найбільш ефективну підтримку бізнесу та ризиків управління.

1. Cloud Access Security Brokers

Програмне забезпечення як послуга (SaaS), які все більш поширені на підприємствах, надають нові виклики для груп безпеки з їх обмеженими можливостями видимості та контролю. Хмари Брокери безпеки доступу (CASB) дозволяють керівникам інформаційної безпеки (CISO) а можливість застосовувати корпоративні політики безпеки до кількох хмарних сервісів.

2. Виявлення кінцевої точки та відповідь

Рішення виявлення та реагування кінцевих точок (EDR) дозволяють CISO виявляти потенціал порушення безпеки та швидко реагувати. Ці інструменти записують події кінцевої точки та мережі, і дані безперервно шукаються за допомогою відомих індикаторів компромісу (IOC) і методи машинного навчання для раннього виявлення порушень.

3. Підходи без сигнатур для запобігання атаки кінцевій точки

Такі методи, як захист пам'яті та запобігання експлуатації, а також машинне навчання на основі систем, які використовують математичні моделі, доповнюють неефективні сигнатурні підходи для запобігання зловмисному програмному забезпеченню проти розширених і цілеспрямованих атак.

4. Поведінкова аналітика користувачів і сутностей

Поведінкова аналітика користувачів і сутностей (UEBA) надає поряд з користувачами орієнтовану аналітичну інформацію про мережі, кінцеві точки та програми. Співвідношення цих аналітик пропонує більш ефективне та точне виявлення загроз.

5. Мікросегментація та видимість потоку

Мікросегментація, більш детальна сегментація, зупиняє зловмисників, які вже знаходяться в системі від переміщення збоку («схід/захід») до інших систем. Інструменти візуалізації забезпечують безпеку команди, щоб зрозуміти моделі потоків, встановити політику сегментації та відстежувати відхилення. Для даних у русі, деякі постачальники надають додаткове шифрування мережевого трафіку.

6. Тестування безпеки для DevOps

Оскільки DevOps інтегрує безпеку в робочий процес (DevSecOps), що розвивається, моделі пропонують автоматизовану, прозору та відповідну конфігурацію базової інфраструктури безпеки на основі політики, що відображає поточний стан робочого навантаження.

7. Рішення для оркестрування операційного центру безпеки, орієнтовані на розвідку

Операційні центри безпеки, керовані розвідками (ISOC), призначені для боротьби з новими парадигмами «виявлення та реагування». Це рішення вимагає розвитку традиційного центру безпеки (SOC), щоб запропонувати адаптивну архітектуру та контекстно-залежні компоненти.

8. Віддалений браузер

CISO можуть звертатися зі зловмисним програмним забезпеченням, що надходить електронною поштою, URL-адресами або веб-сайтами ізоляції функції перегляду від кінцевої точки та корпоративної мережі. Це зроблено шляхом віддаленого представлення сеансу браузера з локального або хмарного сервера. Сеанси сервера можна скинути до відомого справного стану, і ця методика зменшує площу поверхні для атаки, перекладаючи ризик на сеанси сервера.

9. Обман

Інструменти для обману, як випливає з назви, використовують обман або прийоми, щоб запобігти атакам. Команда безпеки створює підроблені вразливості, системи, загальні ресурси та файли cookie, щоб спокусити зловмисників. Будь-яка реальна атака на ці ресурси вказує командам безпеки на атаку, а законні користувачі не побачать і не потребуватимуть доступу до підроблених систем.

10. Повсюдні довірчі послуги

Моделі безпеки повинні розвиватися разом із прогнозованою поширеністю Інтернету Речі (IoT) і зростанням залежності від операційних технологій. Довірчі служби можуть управляти потребами мільярдів пристроїв з обмеженими можливостями обробки. Важливо те, що довірчі служби розроблені для масштабування та можуть запропонувати цілісність, конфіденційність, ідентифікація пристроїв та автентифікацію [5].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ТЕХНОЛОГІЧНИХ ДАНИХ НА БАЗІ IBM GUARDIUM

IBM® Guardium® запобігає витоку з баз даних, сховищ даних і великих даних середовища, такі як Hadoop, забезпечує цілісність інформації та автоматизує контроль відповідності в гетерогенних середовищах. Він захищає структуровані та неструктуровані дані в базах даних, середовищах великих даних і файлах системи проти загроз і забезпечує відповідність. Він забезпечує масштабовану платформу, яка забезпечує постійний моніторинг структурованих і неструктурований трафік даних, а також застосування політики для доступу до конфіденційних даних по всьому підприємству.

Захищений централізований репозиторій аудиту в поєднанні з інтегрованим робочим процесом. Платформа автоматизації оптимізує діяльність перевірки відповідності в широкому діапазоні мандатів. Він використовує інтеграцію з управлінням IT та іншими рішеннями для управління безпекою, щоб забезпечити комплексний захист даних на підприємстві. Вони призначені для забезпечення безперервного моніторингу гетерогенної бази даних і інфраструктури обміну документами, а також забезпечення виконання ваших політик щодо конфіденційного доступу до даних по всьому підприємству з використанням масштабованої платформи. Централізований аудит репозиторію, розроблений для максимальної безпеки в поєднанні з інтегрованою відповідністю.

Додаток для автоматизації робочого процесу дозволяє продуктам оптимізувати відповідність діяльності з підтвердженням за широким спектром мандатів.

IBM Security Guardium розроблено для захисту критичних даних. Гардіум - це комплексна платформа захисту даних, яка дозволяє командам безпеки автоматично аналізувати те, що відбувається в середовищах конфіденційних даних (бази даних, сховища даних, платформи великих даних, хмарні середовища, файлові системи тощо), щоб мінімізувати ризики, захищати конфіденційні дані від внутрішніх і зовнішніх загроз і легко адаптуватися до IT змін, які можуть

вплинути на безпеку даних. Guardium допомагає забезпечити цілісність інформації в центрах обробки даних і автоматизувати контроль за дотриманням вимог.

Рішення IBM Security Guardium пропонується у двох версіях:

- Моніторинг активності бази даних IBM Security Guardium (DAM)
- IBM Security Guardium File Activity Monitoring (FAM) – використовуйте Guardium моніторинг активності для розширення можливостей моніторингу на файлові сервери.

Продукти IBM Guardium забезпечують просте, надійне рішення для запобігання витоку даних з баз даних і файлів, що допомагає забезпечити цілісність інформації в дата-центрі і автоматизацію контролю за дотриманням вимог.

Продукти Guardium можуть допомогти вам:

- Автоматично знаходити бази даних, відкривати й класифікувати конфіденційну інформацію всередині них;
- Автоматично оцінювати вразливості бази даних і недоліки конфігурації;
- Переконатися, що конфігурації заблоковані після внесення рекомендованих змін) реалізовано;
- Увімкнути високу видимість на детальному рівні в транзакціях бази даних, які включають конфіденційні дані;
- Відстежувати діяльність кінцевих користувачів, які опосередковано отримують доступ до даних через додатки;
- Відстежувати та впроваджувати широкий спектр політик, включаючи доступ до конфіденційних даних, контроль змін у базі даних і дії привілейованих користувачів;
- Створення єдиного безпечного централізованого репозиторію аудиту для великої кількості людей гетерогенної системи та бази даних;
- Автоматизування всього процесу аудиту відповідності, включаючи створення та розповсюдження звітів, а також збирання коментарів і підписів.

Рішення Guardium розроблено для простоти використання та масштабованості. Його можна налаштувати для однієї бази даних або тисяч гетерогенних баз даних, розташованих по всьому світу.

Це рішення доступне як попередньо налаштовані пристрої, що постачаються компанією IBM, або як програмне забезпечення приладів, встановлених на вашій платформі. Додаткові функції можна легко додати до вашої системи після установки.

Ось ключові функціональні області рішення безпеки баз даних Guardium:

- Оцінка вразливості. Це включає не тільки відкриття відомої вразливості в продуктах баз даних, а також забезпечення повної видимості складної інфраструктури баз даних, виявлення неправильних конфігурацій та оцінка і пом'якшення цих ризиків.
- Відкриття та класифікація даних. Хоча сама класифікація не передбачає будь-який захист, він служить першим важливим кроком до визначення належної безпеки політики для різних даних залежно від їх критичності та відповідності вимоги.
- Захист даних. Guardium адресує статичне шифрування даних у стані спокою та передачі, динамічне маскування даних, а також інші технології для захисту цілісності даних та конфіденційність.
- Моніторинг і аналітика. Це включає моніторинг продуктивності бази даних, характеристику та повну видимість у всіх доступах та адміністративних діях для кожного екземпляру. Крім того, розширена аналітика в реальному часі, виявлення аномалій а також інтеграція інформації про безпеку та керування подіями (SIEM).
- Керування доступом. Це виходить за рамки базового контролю доступу до бази даних. Процес рейтингування був зосереджений на більш складних, динамічних, політичних управліннях доступом на основі, що здатне ідентифікувати та видалити зайві привілеї користувачів, керування загальними та службовими обліковими записами, а також виявлення та блокування підозрілих дій користувачів.

- Аудит і відповідність. Це включає розширені механізми аудиту власних можливостей, централізований аудит та звітність у кількох базах даних середовища, що забезпечують поділ обов'язків, а також інструменти, що підтримують криміналістичну експертизу аналізу і аудиту відповідності.
- Продуктивність і масштабованість. Хоча сама по собі вона не є функцією безпеки, вона є вирішальною вимогою до того, щоб усі рішення безпеки баз даних могли витримувати високі навантаження, мінімізувати витрати на продуктивність і підтримувати розгортання в режимі високої доступності конфігурації [4].

2.1. Призначення можливості та функції IBM GUARDIUM

IBM Security Guardium Data Protection автоматично знаходить та класифікує конфіденційні дані для всіх корпоративних систем, що забезпечують операції з даними в режимі реального часу та поглиблений аналіз дій користувачів для виявлення нетипових дій з конфіденційними даними. Використання цього рішення дозволить виявляти регулювані дані в сховищах даних і використовувати готові шаблони для таких нормативних вимог, як PCI, SOX, HIPAA, CCPA та багатьох інших, в метою спрощення і автоматизації процесів нормативного контролю.

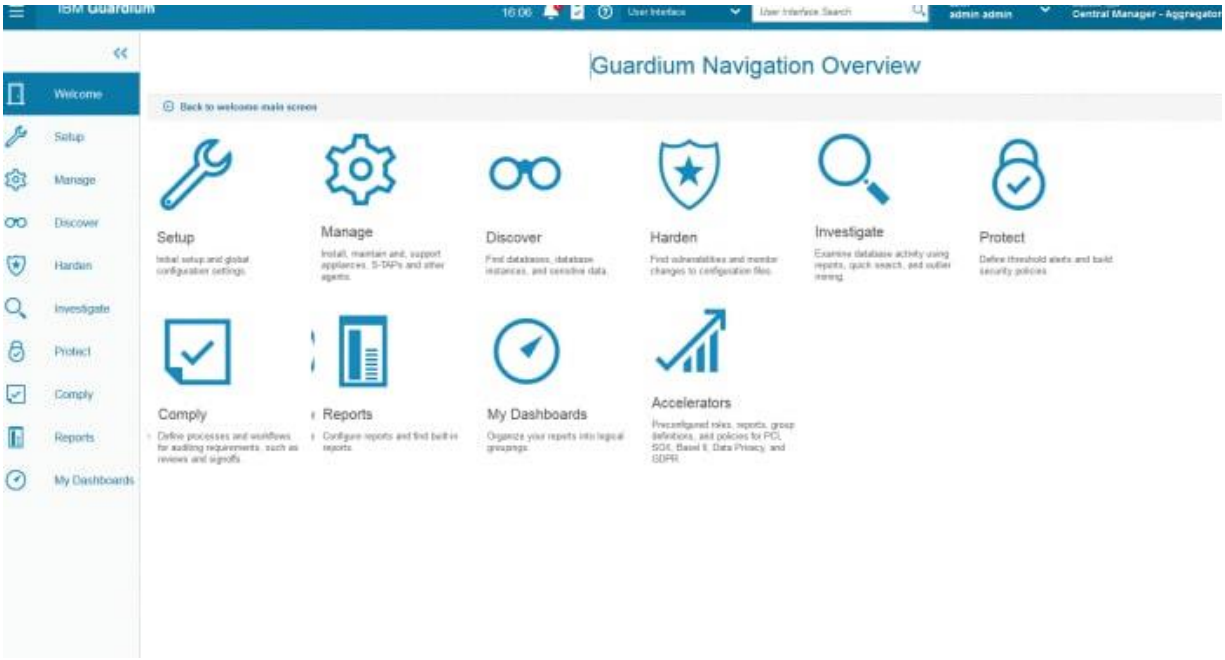

Рис. 2.1. Оглядова вкладка IBM Guardium

Управління доступом до конфіденційних даних.

В основі захисту даних Guardium лежить масштабна архітектура, що забезпечує повний контроль за операціями зі структурованими, напівструктурованими та неструктурованими даними для всіх основних сховищ даних, розташованих локально, в приватних і публічних хмарних середовищах або в контейнерах. Через один інтерфейс можна налаштувати політику доступу, відстежити доступ користувачів до захищених даних, а також виявляти, аналізувати та усувати вразливості та загрози в режимі реального часу у всьому середовищі зберігання даних. Розкриття внутрішніх і зовнішніх ризиків Автоматичний пошук і класифікація конфіденційних даних (в базах і сховищах даних). Моніторинг і аудит всіх дій з даними с Використання когнітивної аналітики та аналітики для виявлення загроз. Призначення політики безпеки в реальному часу Політики безпеки в режимі реального часу захищають дані в масштабах всього підприємства — для всіх операцій доступу за даними, спостереження змін і дій користувачів.

Створення централізованого сховища для всіх даних

Об'єднання всіх даних аудиту в централізованому уніфікованому зберігає для забезпечення відповідності нормативно-правовими вимогами, створення звітів і проведення експертизи. Захист конфіденційних даних в різних гетерогенних середах.

Основні можливості IBM Guardium Data Protection для баз даних:

– Моніторинг і аудит всіх дій з даними, прискорення процедури контролю і отримання нормативів

– Швидка адаптація к змінам в середовищі даних

– Призначення політики безпеки в реальному часу, підтримка гетерогенних середовищ

– Інтеграція з IT-середовищем та екосистемою безпеки організації

2.2. Можливості щодо адміністрування системи IBM GUARDIUM

- Завдання керування включають моніторинг працездатності вашої системи та керування такими артефактами як групи, домени та сповіщення.
- Адміністратори Guardium® здійснюють різноманітне адміністрування та обслуговування завдання.
- Установіть сертифікати, щоб ви могли підключитися до графічного інтерфейсу Guardium, а також до Guardium-S-
- TAP® зв'язок. Регулярно перевіряйте сертифікати, щоб ви могли оновлювати їх до їх закінчення.
- Сповіщення
- Продуктивність і моніторинг системи

Навчіться використовувати інструменти Guardium для підтримки продуктивності системи: використання одиниць звітів для виявлення недостатньо і надмірно використовуваних систем; самоконтроль системи; і сторінку стану послуг

- Планування

Планувальник загального призначення використовується для планування багатьох різних типів завдань (архівування, агрегація, автоматизація робочого процесу тощо)

- Псевдоніми

Створіть синоніми для значення даних або об’єкта, які будуть використовуватися у звітах або запитах.

- Дати та позначки часу

Використовуйте інструмент календаря, щоб вибрати точну дату, і інструмент вибору відносної дати, щоб вибрати дату, яка відноситься до поточного часу.

- Періоди часу будівництва

Правила політики та умови запиту можуть перевірити події, які відбуваються (або ні) під час визначення користувачем періодів часу.

- Шифрові набори

Набори шифрів — це комбінації криптографічних параметрів, які визначають алгоритми безпеки та розміри ключів.

• Коментарі

Коментарі застосовуються до визначень і результатів робочого процесу.

• Завантаження клієнтів

Служба підписки на захист бази даних підтримує обслуговування попередньо визначених тестів оцінки, тести на основі SQL, CVE, APAR та групи, такі як версії баз даних і виправлення.

• Передайте дані Guardium в іншу програму

Використовуйте потокове передавання даних, щоб надсилати трафік, зібраний Guardium, на інший інструмент для аналізу.

• Розвідка великих даних

Платформа Guardium Big Data Intelligence (GBDI) зберігає зібрані дані більш тривалі терміни, забезпечуючи прямий доступ майже в режимі реального часу до безпеки даних і звіти про відповідність вимогам.

• Експорт та імпорт визначень

Використовуйте визначення експорту та імпорту, якщо у вас є кілька систем з ідентичними або аналогічними вимогами і не використовується центральне управління. Ви можете визначити компоненти, які вам потрібні в одній системі, і експортуйте ці визначення в інші системи, які знаходяться на одному рівні випуску програмного забезпечення.

• Віддалені реєстратори

Перегляньте правила пересилання для віддаленого реєстратора та перевірте з’єднання.

• Керуйте користувацькими класами

Завантажуйте та підтримуйте спеціальні класи, які використовуються в попередженнях або оцінках.

• Готовність до GDPR: міркування під час налаштування Guardium

Дізнайтеся, як дані персональної ідентифікаційної інформації (PII) зберігаються на вашому пристрої системи Guardium і як ними керувати.

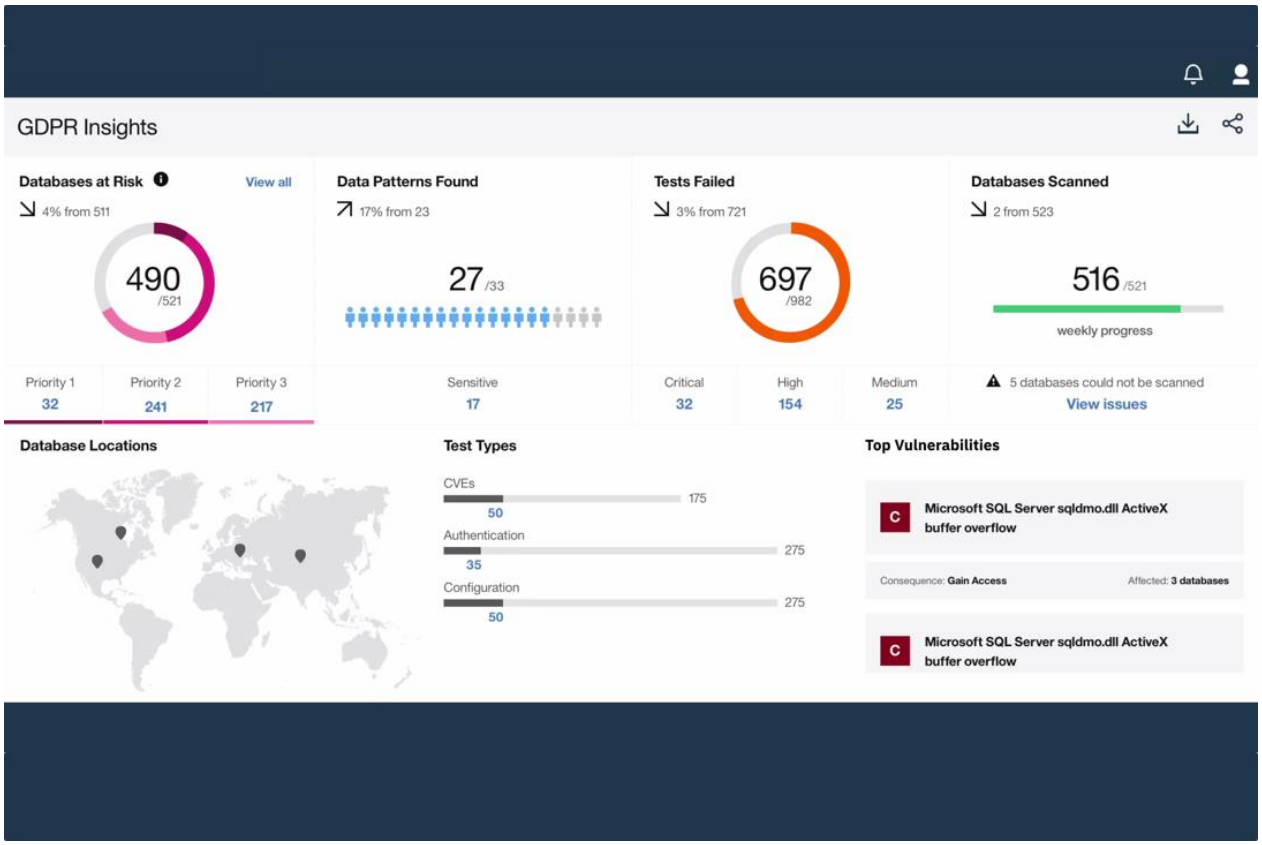

Рис. 2.2. Захист відповідно до GDPR у IBM Guardium

Групи

Використання груп дозволяє легко створювати класифікатор, політику та запит і керувати ними, а також розгортати оновлення для ваших клієнтів S-TAP і GIM. Скоріше ніж необхідність багаторазово визначати групу об'єктів даних для політики доступу, додайте об’єкти в групу, щоб легко керувати ними.

- Ролі безпеки

Ролі безпеки використовуються для надання доступу до даних (груп, запитів, звітів тощо) і для надання доступу до програм (конструктор груп, конструктор запитів-звітів, політика Builder, CAS, оцінки безпеки тощо).

- Як встановити патчі

Встановіть один або кілька патчів як фоновий процес.

- Технічне обслуговування

Функція підтримки захищена паролем і може використовуватися лише під керівництвом технічної підтримки [12].

- Центральне управління

У конфігурації центрального управління один блок Guardium® позначається як центральний менеджер. Цей блок можна використовувати для моніторингу та керування іншими підрозділами Guardium, які називаються керованими

Некеровані одиниці називаються окремими одиницями.

Концепція локальної системи Guardium може посилатися на будь-яку систему Guardium в парадигмі центрального управління. Деякі програми (процеси аудиту, запити, портрети тощо) можна запускати як на керованих блоках, так і на центральному менеджері. В обох випадках визначення надходять від центрального менеджера, а дані — від локальної системи Guardium (яка також може бути центральним менеджером).

Після налаштування центральної системи керування ви можете використовувати центральний менеджер або керований блок для створення або зміни більшості визначень. Майте на увазі, що більшість визначень зберігаються в центральному менеджері, незалежно від системи, яка виконує фактичне редагування.

За допомогою функції віддаленого джерела користувач менеджера може: запускати будь-який звіт на керованому блоці (користувач повинен мати правильні повноваження ролі); і переглядати дані та інформацію цього керованого підрозділу.

Визначення шаблонів CAS спільно використовують усі підрозділи об’єднаного середовища, як і всі інші визначення (звіти, політики, сповіщення тощо).

Рекомендується, щоб користувач запускав звіти CAS на менеджері, особливо звіти CAS, що стосуються конфігурацій CAS, хостів і шаблонів.

Якщо ви створюєте звіт за допомогою конструктора спеціального домену, а деякі або всі таблиці є віддаленими (вони зберігаються в менеджері, наприклад, джерело даних або коментарі), цей звіт не працюватиме на керованому вузлі. Дані не повертаються.

Сторінка центрального керування менеджера не оновлюється автоматично за певним інтервалом. Час очікування залежить від часу очікування графічного інтерфейсу системи.

Через деякий час бездіяльності система автоматично вийде з системи та відобразить діалогове вікно входу. Тривалість тайм-ауту GUI можна встановити за допомогою тайм-ауту сеансу зберігання команд CLI (за замовчуванням 900 секунд). Перегляньте час очікування за допомогою команди CLI show session timeout. Індикатори стану оновлюються кожні 5 хвилин, коли сеанс активний.

Щоб синхронізувати або завантажити будь-які дані з центрального диспетчера на керовані вузли, усі вузли, які задіяні в цьому типі діяльності, повинні бути в одній версії Guardium.

Під час переходу із резервуванням центрального управління може знадобитися до 5 хвилин для синхронізації типу блоку залежно від того, скільки одиниць визначено в середовищі центрального керування.

Інформація IPMODE передається центральному менеджеру під час реєстрації. Керований блок, який зареєструвався в центральному менеджері у версії до V11.2, не знає про свій IP-режим і не може поділитися цією інформацією з центральним менеджером. Навіть якщо керований блок було оновлено до V11.2 або новішої, він не ділиться своїм IP-режимом з центральним менеджером, якщо ви не скасуєте реєстрацію та повторно зареєструєте його. Щоб виправити: На сторінці Central Manager виберіть окремі керовані одиниці або всі керовані одиниці та натисніть оновити інформацію про блок [17].

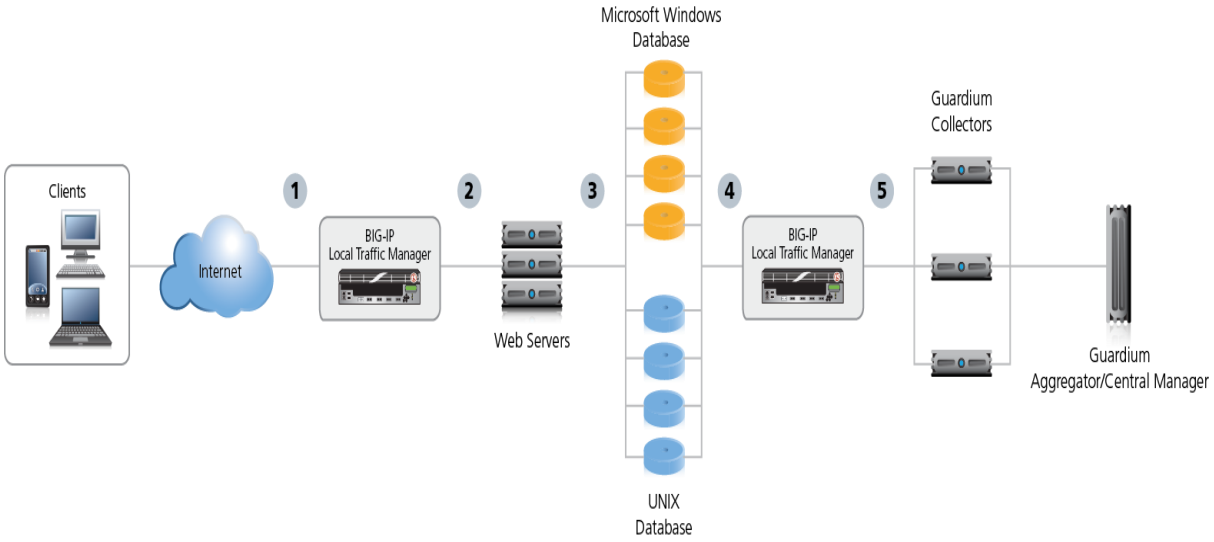

Рис. 2.3. Структура рішення IBM GUARDIUM га основі Central Manager

Служби компонентів Guardium

Визначте компоненти Guardium та розташування, з яких вони взяті в середовищі центрального керування.

Цей блок можна використовувати для моніторингу та керування іншими підрозділами Guardium, які називаються керованими. Некеровані одиниці називаються окремими одиницями.

Користувачі, ролі безпеки, визначення процесу аудиту та групи експортуються з центрального менеджера до всіх керованих підрозділів за розкладом, як описано далі.

З центрального менеджера адміністратор може:

- Зареєструвати підрозділи Guardium для управління;
- Відстежувати керовані блоки (наявність блоку, стан двигуна інспекції тощо);
- Переглядати файли системного журналу (системних журналів) керованих блоків;
- Переглядати звіти за допомогою даних про керовані одиниці;
- Переглядати основну статистику для керованих підрозділів;
- Установити політики безпеки Guardium на керованих блоках;
- Перезапустити керовані блоки;
- Керувати інспекційними механізмами Guardium на керованих блоках;
- Підтримувати повний набір дозволів користувачів, ролей безпеки, груп і ролей програми, які використовуються в усіх керованих системах;
- Розповсюджувати патчі;
- Розповсюджувати завантажені файли JAR;
- Розповсюджувати параметри резервного копіювання виправлень;
- Розповсюджувати конфігурацію аутентифікації;
- Розповсюджувати конфігурації.

Примітка. Дозволи на роль програми також може змінювати адміністратор з будь-якого керованого блоку. Коли це станеться, дозволи змінюються для всіх керованих блоків [18].

Впровадження центрального керування в новій інсталяції

Зробіть одну машину центральним менеджером, використовуйте той самий загальний секрет, реєструйте одиниці та керовані групи.

Зробіть одну машину центральним менеджером

Перше, що потрібно виконати, це зробити з однієї машини центральний менеджер. Виберіть машину. Потім виконайте наступні кроки. Увійдіть до CLI машини, яку ви хочете зробити центральним менеджером. Введіть менеджер типів магазину. Цей крок робить машину центральним менеджером; однак вона ще нічим не керує. Використовуйте Same Shared Secret

Після того як у вас є центральний менеджер, ви повинні підключити інші машини до центральної системи керування. З міркувань безпеки необхідно, щоб зв'язок між машинами був зашифрований з використанням одного спільного секрету. Щоб виконати цей крок, виконайте наведені нижче дії.

Натисніть Налаштування > Інструменти та подання > Система, щоб відкрити Систему.

Встановіть для загального секрету один і той же рядок у всіх системах [19].

Реєстраційні одиниці

Зареєструйте керовані одиниці для зв'язку з центральним менеджером.

Ви можете зареєструвати одиниці Guardium для центрального керування або з центрального менеджера, або з самого пристрою. Незалежно від того, як виконується реєстрація, центральний менеджер і всі керовані підрозділи повинні мати один і той самий загальний системний секрет. Якщо підрозділ, яким потрібно керувати, вже зареєстровано для центрального керування іншим менеджером, скасуйте реєстрацію підрозділу у цього центрального менеджера, перш ніж зареєструвати його у нового менеджера. Обов'язково зрозумійте, що саме відбувається з цим підрозділом, коли він зареєстрований і не зареєстрований для центрального управління.

Якщо користувач, який увійшов до керованого блоку, не існує в центральному менеджері, сеанс стає недійсним. Він залишається недійсним, доки підрозділ не буде зареєстрований у центрального менеджера.

Що відбувається під час реєстрації

При реєстрації відбуваються наступні дії.:

- Тип пристрою встановлюється на керований, а IP менеджера зберігається.
- Застосовано ключ продукту менеджера. (Ліцензійний ключ не передається за допомогою Ping або синхронізації користувача.
- Він надсилається під час реєстрації або під час оновлення системи. Усі планування завдань скинуто до стандартних.
- Усі файли psml (налаштування графічного інтерфейсу порталу) видаляються.
- Усі локальні користувачі та ролі видаляються.
- Список порогових попереджень, які не оцінюються, скидається.
- Завантажуються ролі користувачів, дозволи від менеджера.
- Завантажуються спеціальні класи, файли JAR, завантажені користувачем, довірче сховище LDAP від менеджера.
- З'єднання з базою даних від керованого до менеджера ввімкнено.
- З'єднання з базою даних від менеджера до керованого ввімкнено. За потреби запускається прослуховувач CAS.
- Після реєстрації всі визначення звітів, запитів, груп, політик, аудитів тощо витягуються з центрального менеджера.
- Якщо статус зареєстрованого пристрою залишається офлайн
- Якщо ви знаєте, що зареєстрований пристрій перебуває в режимі онлайн і доступний із центрального менеджера, але його статус залишається офлайн, виконайте наступні кроки.
- Переконайтеся, що пристрій, яким потрібно керувати, перебуває в режимі онлайн, доступний і працює, за допомогою вікна браузера для входу в систему Guardium на цьому пристрої.
- Натисніть Оновити для пристрою. Переконайтеся, що ви ввели правильну IP-адресу для пристрою.
- Перевірте, чи блок має той самий спільний секрет, що й центральний менеджер.

- Якщо реєстрація блоку не в мережі, запит на реєстрацію зберігається. Він повторно надсилається на IP/порт, зазначений через встановлений інтервал, доки пристрій не зареєструється.
- Термін дії запиту на реєстрацію, який не виконано, закінчується через сім днів.
- Реєстрація з керованого підрозділу На керованому блоці ви можете використовувати графічний інтерфейс для реєстрації пристрою в центральному менеджері.
- В іншому випадку ви можете використовувати команду реєстру CLI, як описано в розділі
- Реєстрація керованого блоку за допомогою CLI. Натисніть Налаштування > Центральне керування > Реєстрація та баланс навантаження, щоб відкрити реєстрацію центрального керування.
- Для IP-адреси хосту введіть IP-адресу центрального менеджера.
- Для порту введіть https порт для центрального менеджера (зазвичай 8443). Натисніть Зареєструвати.
- Після реєстрації в керованому блоці він ініціює зв’язок із центральним менеджером, і більше нічого робити не потрібно. Центральний блок управління має бути в режимі онлайн та доступним для цього підрозділу, коли ви реєструєтеся для центрального управління.
- На відміну від цього, коли ви реєструєте одиниці для управління з центрального блоку управління, ви можете зареєструвати одиниці, які зараз недоступні.
- Реєстрація керованого блоку за допомогою CLI На керованому блоці увійдіть у CLI. Введіть управління реєстром <IP менеджера> <Порт менеджера> Після реєстрації в керованому блоці він ініціює зв’язок із центральним менеджером, і більше нічого робити не потрібно.
- Реєстрація одиниць з центрального менеджера Ви можете зареєструвати одиниці, які зараз недоступні. Перейдіть до Керування > Центральне керування > Центральне керування, щоб відкрити центральне керування. Натисніть Зареєструвати новий.

- Відкриється сторінка реєстрації блоку. Введіть IP-адресу та порт пристрою та натисніть Зберегти. Сторінка центрального керування оновиться з новим блоком [16].

Адміністрація Guardium®

Адміністратори Guardium® виконують різні завдання адміністрування та обслуговування.

Будь-який користувач, якому призначено роль адміністратора, називається адміністратором Guardium. Це відрізняється від облікового запису адміністратора. Роль адміністратора Guardium відповідає за використання ідентифікаторів адміністратора та CLI у виробничих системах.

Привілеї ролі адміністратора

Роль адміністратора Guardium має привілеї, які не призначаються цій ролі явно. Наприклад, коли користувач із роллю адміністратора відображає список визначень набору конфіденційності, усі набори конфіденційності, визначені в системі Guardium, відображаються, а користувач із роллю адміністратора може переглядати, змінювати або видаляти..

Коли користувач без ролі адміністратора отримує доступ до списку наборів конфіденційності, цей користувач бачить лише ті набори конфіденційності, якими він або вона володіє (тобто створені), а також усі набори конфіденційності, яким було призначено роль безпеки, яка також призначена цьому користувачеві.

CLI diag Командний доступ

Використання команди CLI diag вимагає додаткового пароля, який може бути паролем будь-якого користувача з роллю адміністратора.

Якщо ввімкнено автоматичне блокування облікового запису (функція, яка блокує обліковий запис користувача після певної кількості помилок входу), обліковий запис користувача адміністратора може бути заблоковано після кількох невдалих спроб входу. Якщо це станеться, скористайтеся командою unlock admin CLI, щоб розблокувати його.

Менеджер доступу (accessmgr) може розблокувати облікові записи з браузера користувачів. Відкрийте браузер користувача, натиснувши Access > Access Management > User Browser.

Права користувача адміністратора

Користувач-адміністратор має додаткові привілеї, які не надаються ролі адміністратора, а саме:

- Доступ до списків справ усіх користувачів;
- Власник імпортованих визначень;
- Функції керування доступом;
- Повноваження списку справ адміністратора.

Список справ — це функція автоматизації робочого процесу, яка контролює розподіл результатів процесу аудиту серед користувачів. Адміністратор має спеціальні привілеї та обов'язки в цій сфері. Якщо обліковий запис користувача вимкнено, усі результати процесу аудиту для цього користувача будуть автоматично перепризначені користувачеві з адміністратором. Якщо користувач недоступний з будь-якої іншої причини, результати процесу аудиту можуть бути встановлені в списку справ цього користувача, тобто в очікуванні підписання, перш ніж передаватись наступному одержувачу результатів. Користувач-адміністратор може відкрити список справ будь-якого користувача та виконувати будь-які дії, доступні цьому користувачу. Коли користувач-адміністратор виконує будь-які дії зі списком справ іншого користувача, цей факт зазначається в журналі діяльності процесу аудиту, наприклад, результати, підписані адміністратором користувача від імені користувача x.

Власність імпортованого визначення

Коли визначення експортуються, усі ролі видаляються, а власник змінюється на користувача-адміністратора. Це єдиний спосіб контролювати, як визначення використовуватиметься в системі імпорту.

Керування доступом і адміністратор

З міркувань безпеки передбачено розділення обов'язків менеджера доступу та адміністратора. Користувачі-адміністратори не можуть мати привілеї менеджера доступу, і навпаки.

Наступного разу, коли користувач-адміністратор увійде в систему, йому буде доступна функція менеджера доступу. Це можливо лише для адміністратора (а не для інших користувачів, які мають роль адміністратора).

Один і той самий користувач може мати обидві ці ролі через. Однак поточне використання не дозволить призначати дві ролі одному користувачеві.

Раніше, коли пристрій оновлювався, роль accessmgr призначалася користувачеві адміністратора, а користувач accessmgr був вимкнений.

У цій ситуації, щоб налаштувати accessmgr і admin, увійдіть як адміністратор і ввімкніть користувача accessmgr, а потім увійдіть як accessmgr (початковий пароль за замовчуванням isguardium) і видаліть роль accessmgr від користувача адміністратора [13].

Повідомлення

Використовуйте Alert і Alert Builder для створення сповіщень. Якщо для дій попередження потрібні електронна пошта або інші сповіщення, виконайте цю процедуру для кожного типу сповіщень, які потрібно визначити.

Конфігурація оповіщення

- Перш ніж вибрати дії попередження, ви повинні налаштувати параметри SMTP електронної пошти в Alerter
- Відкрийте оповіщення, натиснувши Захист > Виявлення вторгнення в базу даних > Оповіщення.
- Заповніть інформацію SMTP та/або SNMP.
- Після заповнення кожного розділу натисніть Перевірити з’єднання та переконайтеся, що з’єднання працює. Ви отримаєте повідомлення про те, що з’єднання недоступне, якщо з’єднання не працює.
- Натисніть Застосувати, щоб зберегти конфігурацію.
- Принаймні необхідно вказати IP-адресу/ім’я хоста, порт та зворотну адресу електронної пошти.
- Виберіть Пошта в меню Тип сповіщення. Якщо серйозність повідомлення ВИСОКА, встановлюється прапорець терміново.
- Виберіть користувача (яким може бути особа або група) зі списку одержувача сповіщень. Додатковими одержувачами сповіщень електронною поштою в режимі реального часу є Invoker (користувач, який ініціював фактичну команду SQL, яка спричинила запуск політики) і Owner (власник/власники бази даних). Ідентифікація Invoker і власника здійснюється шляхом отримання

ідентифікаторів користувачів (на основі IP), налаштованих за допомогою API Guardium®.

- Натисніть Додати.
- Створіть оповіщення
- Після налаштування оповіщення відкрийте конструктор сповіщень, натиснувши Захист > Виявлення вторгнення в базу даних > Конструктор сповіщень.
- Заповніть інформацію в розділах «Налаштування», «Визначення сповіщення», «Порогове значення» та «Повідомлення» та натисніть «Застосувати».
- Виберіть, хто отримуватиме сповіщення, натиснувши Додати одержувача та вибравши користувача [14].

Огляд груп

Згрупуйте подібні об’єкти даних і використовуйте їх у створенні визначень запитів, політики та класифікації. Використовуйте одну з багатьох попередньо визначених груп або створіть власну групу за допомогою Конструктора груп.

Є багато місць, де групи практично використовувати. Групуючи подібні об’єкти даних, ви можете використовувати весь набір об’єктів у політиках, класифікаціях та запитах, замість того, щоб вибирати декілька об’єктів даних окремо.

Якщо вам потрібно змінити запит або політику, а не застосовувати ці зміни до кожного окремого об’єкта, ви можете застосувати ці зміни до групи.

S-TAP і GIM також використовують групи, щоб полегшити розгортання оновлень на керованих серверах.

Конструктор груп

Використовуйте конструктор груп, щоб створити нову групу або змінити існуючу групу з інтерфейсу користувача.

Щоб відкрити Конструктор груп, натисніть Налаштування > Конструктор груп. Використовуйте екран «Груповий фільтр», щоб сортувати групи за типом програми, типом групи, описом або категорією.

Типи груп

Поле Тип групи відноситься до типу даних, які можна згрупувати. Наприклад, IP-адреса сервера очікує дані, відформатовані як IP-адреса, а користувачі очікують побачити імена користувачів у програмі.

Групи кортежів

Група кортежів дозволяє об’єднати декілька атрибутів разом, щоб утворити єдиний складений член групи. Кортежи можуть допомогти спростити визначення умов для звітності та правил політики. Три з впорядкованого набору значень називаються 3-кортежними. n-кортеж — це кортеж із n-набором атрибутів значень.

Прикладами груп кортежів є:

- Групи кортежів: Об'єкт/Команда, Об'єкт/Поле, Користувач IP-адреси клієнта/БД, IP-адрес сервера/Користувач БД;
- 3-кортежні групи: IP-адреса клієнта/джерела програми/користувач БД, користувач БД/об’єкт/привілей;
- Група з 5 кортежів: IP-адреса клієнта/джерела програми/користувач БД/IP-адреса сервера/примірник служби;
- Група з 7 кортежів: IP-адреса клієнта/Src App/DB Користувач/IP-адрес сервера/Svc. Ім’я/Користувач ОС/Ім’я БД;

Використовуйте косу риску (/), щоб розділити значення в кортежі. Ви можете вказати багато елементів кортежу за допомогою символу підстановки (%).

У запиті на кортеж, якщо ваші дані містять зворотну косу риску (\ ), а ви вказуєте LIKE GROUP, результат може бути неправильним. Якщо дані містять зворотну косу риску, замість цього використовуйте IN GROUP.

Попередньо визначені групи

Існує ряд попередньо визначених груп, які входять до складу Guardium. Використовуйте меню «Фільтр групи» та «Тип групи», щоб переглянути список груп і знайти ту, яка найкраще відповідає вашим потребам.

Типи груп DB User/DB Password за замовчуванням доступні лише користувачам-адміністраторам. Змініть ролі груп, якщо ви хочете змінити це налаштування за замовчуванням.

Перекриття членства в групах

Учасники груп можуть бути в кількох групах.

Наприклад, дві попередньо визначені групи, команди створення та команди DDL, мають членів з іменами CREATE TABLE. Якщо ви робите запит для будь-якої з цих груп, усі члени CREATE TABLE за звітний період зараховуються до цієї групи.

В деяких випадках. Можна визначити набір груп, щоб кожен член належав лише до однієї групи. Наприклад, припустимо, що для цілей звітності потрібно згрупувати користувачів бази даних в одну з двох груп: співробітники або консультанти. Ви можете визначити кожну з цих груп з однаковим типом підгрупи (наприклад, «Статус працівника»). Коли використовуються підгрупи, ви не можете додати учасника до підгрупи, якщо цей учасник уже був доданий до іншої групи з таким самим типом підгрупи.

Підстановки в членах

Члени групи можуть включати символи підстановки (%), коли група використовується в умові запиту або правилі політики.

Керовані групи підрозділів

Існує відмінність між керованими групами одиниць і групами, створеними за допомогою конструктора груп, який використовується для групування елементів. Групи, створені за допомогою конструктора груп, допомагають спростити створення політик і керування ними, а також роз’яснення подання звітів. Для більш інформацію про керовані групи підрозділів див. у розділі Створення керованих груп підрозділів [13].

3 ОРГАНІЗАЦІЯ ЗАХИСТУ ДАНИХ КОМПАНІЇ ЗАСОБАМИ IBM GUARDIUM

Для організації захисту даних компанії засобами IBM Guardium необхідно пройти кілька кроків, таких як розпізнавання об'єктів інформаційної системи, які потребують захисту, кастомізації класифікації об'єктів, у разі необхідності, вибір і налаштування засобів розпізнавання атак і протидія їм, налаштування автоматичного розпізнавання рівня ризику для кожної встановленої потенційної загрози, налаштування аудиту і моніторингу необхідних об'єктів, а також попередне налаштування автоматичних звітів. Розглянемо деякі з цих функцій детальніше

3.1. Визначення об’єктів інформаційної системи, що потребують захисту

Джерела даних

Джерела даних зберігають інформацію про вашу базу даних або репозиторій, наприклад тип бази даних, розташування сховища або облікові дані, які можуть бути пов’язані з нею. Ви повинні визначити джерело даних, щоб використовувати його з додатками Guardium®.

Створення визначення джерела даних

Джерело даних — це з’єднання з базою даних, яке створюється та налаштовується для використання Програм Guardium, таких як оцінка вразливості та класифікатор. Джерело даних можна створити за допомогою інструмента визначення джерел даних або шляхом створення та завантаження CSV за допомогою інструмента Завантаження клієнта в інтерфейсі користувача Guardium. Можна також створити джерело даних за допомогою API Guardium.

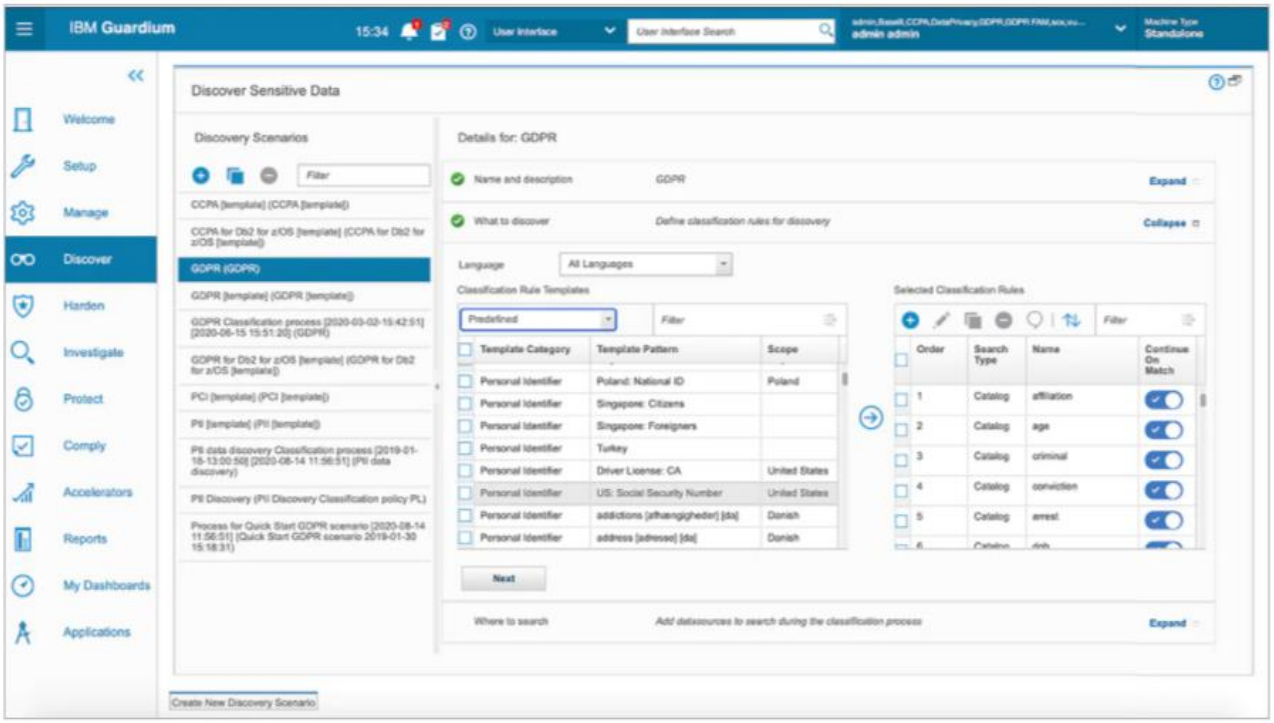

Рис. 3.1. Вкладка пошуку джерел даних

Налаштування джерела даних

Конфігурація залежить від типу бази даних, яку ви використовуєте.

Налаштування спеціальних властивостей для ваших джерел даних

Збільште свої джерела даних, визначаючи та призначаючи власні властивості.

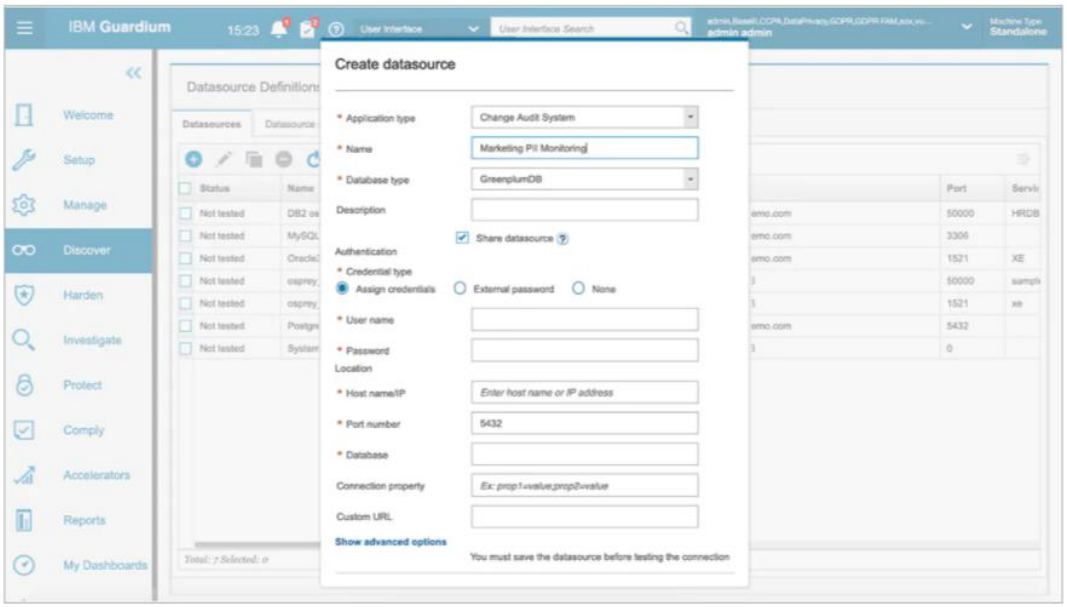

Рис. 3.2. Вкладка створення нового джерела даних

Робота з наявними джерелами даних

Після створення визначення джерела даних ви можете клонувати, змінювати або видаляти файл, джерело даних.

Звітність про джерела даних

Guardium надає звіти про джерела даних, які є у вашому середовищі та будь-які внесені до них зміни.

Визначення джерела даних за допомогою імені служби

Ви можете визначити джерело даних, яке дозволить вашим користувачам підключатися до бази даних Oracle, використовуючи назву служби за допомогою спеціальної URL-адреси.

Керування визначеннями KDC

Якщо ваше джерело даних вимагає автентифікації за допомогою Kerberos, ви можете вказати інформацію, необхідну Guardium для отримання квитка Kerberos перед тим, як зробити підключення.

Керування обліковими даними джерела даних за допомогою CyberArk

Guardium підтримує постачальник паролів програми CyberArk, надійне рішення для численних проблем(тут була и) з обслуговуванням та безпекою, які виникають під час керування паролями.

Використовуйте CyberArk для безпечного зберігання, надання, аудиту та керування своїм Guardium

Облікові дані джерела даних.

Керування обліковими даними джерела даних за допомогою AWS Secrets Manager

Інтегруйте свою систему Guardium із секретами Amazon Web Services (AWS).

Менеджер для безпечного зберігання, керування, обертання та отримання облікових даних для ваших джерел даних, які використовують службу Amazon Relational Database Service (RDS).

Керування обліковими даними джерела даних за допомогою HashiCorp

Інтегруйте свою систему Guardium з HashiCorp, щоб безпечно зберігати, керувати, обертати та отримати облікові дані для всіх підтримуваних джерел

даних. Ви можете налаштувати свої Guardium системи для автентифікації у сховищі HashiCorp за допомогою імені користувача та пароля

- Безпека транспортного рівня (TLS), автентифікації на стороні сервера за допомогою TLS або на стороні клієнта
- автентифікація за допомогою TLS. Якщо ви використовуєте автентифікацію на стороні клієнта за допомогою TLS, ви повинні
- створіть та імпортуйте підписаний клієнтом сертифікат у всі ваші системи[6]

Створення визначення джерела даних

Джерело даних — це з’єднання з базою даних, яке створюється та налаштовується для використання з додатками Guardium®, такими як оцінка вразливості та класифікатор. А джерело даних можна створити за допомогою інструмента визначення джерел даних або шляхом створення і завантаження файлу CSV за допомогою інструмента Customer Uploads у користувача Guardium інтерфейс. Ви також можете створити джерело даних за допомогою API Guardium.

Перед початком роботи потрібно переконатися, що користувач Guardium має привілеї, необхідні для доступу до бази даних. Щоб призначити користувачеві привілеї доступу до бази даних, адміністратор бази даних повинен завантажити та запустити набір сценаріїв на сервері бази даних.

Процедура

1. Відкрийте інструмент «Визначення джерела даних», натиснувши «Налаштування» > « Інструменти та».

Перегляди > Визначення джерела даних .

2. Перейдіть на вкладку Джерела даних .

3. Натисніть, щоб відкрити вікно Створити джерело даних. Входи змінюються залежно від вашого вибору програми, типу бази даних і джерела даних.

4. Виберіть тип програми .

5. Введіть унікальну назву для джерела даних.

6. У меню Тип бази даних виберіть базу даних або тип файлу.

7. Виберіть Поділитися джерелом даних, щоб поділитися визначенням джерела даних всіх програм Guardium. Якщо джерело даних не є спільним, ви можете використовувати визначення лише для вибраного типу програми.

8. Протокол автентифікації залежить від вашого вибору типу бази даних .

- Виберіть Використовувати SSL та Імпортувати сертифікат SSL сервера . Додати

Опція сертифіката доступна для джерел даних, які підтримують взаємну SSL автентифікацію. Сертифікат для взаємної автентифікації SSL додається після конфігурації джерела даних.

- Щоб використовувати автентифікацію LDAP, виберіть LDAP і приступіть до призначення

облікові дані джерела даних.

- Для Kerberos виберіть попередньо визначену конфігурацію Kerberos
- Конфігурації Kerberos меню і введіть Realm і KDC сервера.
- Порада: щоб перевірити, чи існує конфігурація Kerberos на Guardium
- GUI, перейдіть до Налаштування > Інструменти та представлення > Конфігурація Kerberos .
- створити нову конфігурацію Kerberos, яка визначає ваш KDC і Realm,
- Облікові дані для входу мають бути дійсним ідентифікатором користувача Kerberos та паролем також використовується для центру сертифікації (ЦС). Перевірте свої облікові дані Kerberos
- Переконайтеся, що його можна використовувати для входу в командний рядок Hive beeline.

9. Виберіть відповідний тип облікових даних .

- Виберіть Призначити облікові дані, щоб вручну ввести користувача ім'я та пароль для джерела даних.
- Виберіть Зовнішній пароль, щоб отримати пароль із зовнішнього користувача система управління повноваженнями. Виберіть керування обліковими даними програму з меню Тип зовнішнього пароля .
- Якщо облікові дані не призначені, виберіть Немає .

10. Налаштуйте ім'я хоста/IP- адресу, номер порту , базу даних , з'єднання властивість і спеціальна URL-адреса.

Якщо ви використовуєте систему аудиту конфігурації (CAS), перейдіть на вкладку « Додатково » та налаштуйте екземпляр бази даних CAS.

Порада: вхідні дані відрізняються залежно від типу бази даних, яку ви використовуєте. Для більшої інформації, див Налаштування джерела даних .

11. Необов’язково: перейдіть на вкладку Custom та виберіть властивість зі списку налаштованих значень для призначення джерела даних. Якщо спеціальні властивості не налаштовано, ви можете тимчасово зберегти джерело даних і призначити властивості пізніше. Для більшої інформації див Налаштування спеціальних властивостей для ваших джерел даних.

12. Збережіть джерело даних і перевірте з'єднання. Якщо можливо, додайте взаємний SSL сертифікат автентифікації за допомогою кнопки Додати сертифікат.

Сертифікат — це файл PEM, який містить як закритий ключ, так і файл сертифікат. Ви повинні включити обидва рядки BEGIN та END для приватного ключа та сертифікату. Ви також можете встановити сертифікат за допомогою CLI. Для більшої інформації, див Установка сертифіката приладу.

Коли ви вперше тестуєте з’єднання з джерелом даних SSL, ви можете зіткнутися з такою помилкою:

```
Could not connect to: 'jdbc:db2://hostname:port_number/db_name' for user: 'Your_datasource_name_DB2(Security Assessment)'. DataSourceConnectException: Could not connect to: 'Your_datasource_name_ 123.123.123.123:port_number' for user: 'db2inst1'. Exception: com.ibm.db2.jcc.am.DisconnectNonTransientConnectionException: [jcc][t4][2030][11211][4.15.134] A communication error occurred during operations on the connection's underlying socket, socket input stream.
```

Рис. 3.3. Помилка з’єднання з джерелом даних SSL

Помилка виникає, коли графічний інтерфейс не має правильного файлу сховища ключів для сертифікату, який завантажується в пам'ять. Щоб виправити помилку, перезапустіть графічний інтерфейс та перевірте знову з'єднання.

Ви можете використовувати параметри в меню, щоб перевірити з’єднання для одного або кількох джерел(тут була а) даних, додайте джерела даних до групи та оновіть облікові дані або користувацькі дані, властивості, якщо необхідно.

Налаштування джерела даних

Конфігурація залежить від типу бази даних, яку ви використовуєте.

- Клацніть тип бази даних, щоб переглянути інформацію про конфігурацію вашого джерела даних.
- Amazon Redshift

Налаштуйте джерело даних Amazon Redshift у вашій системі Guardium.

- Астра

Налаштуйте джерело даних Aster у вашій системі Guardium.

- Менеджер Cloudera

Налаштуйте джерело даних Cloudera Manager у вашій системі Guardium.

- Кушетка

Налаштуйте джерело даних Couchbase у вашій системі Guardium.

- DataStax Кассандра

Налаштуйте джерело даних DataStax Cassandra із підключенням DataDirect на своєму Guardium.

- Db2

Налаштуйте джерело даних Db2® у вашій системі Guardium.

- Db2 для i

Налаштуйте джерело даних Db2 for i у вашій системі Guardium.

- Db2 для z/OS

Налаштуйте джерело даних Db2 для z/OS® у вашій системі Guardium.

- GreenplumDB

Налаштуйте джерело даних GreenplumDB у вашій системі Guardium.

- Guardium Big Data Intelligence

Налаштуйте джерело даних Guardium Big Data Intelligence (GBDI) на своєму Guardiumsystem.

- Вулик

Налаштуйте джерело даних Hive у вашій системі Guardium.

- Informix

Налаштуйте джерело даних Informix® у вашій системі Guardium.

- MongoDB

Налаштуйте джерело даних MongoDB у вашій системі Guardium.

- MS SQL Server (DataDirect - динамічний порт)

Налаштуйте джерело даних MS SQL Server у вашій системі Guardium.

- MS SQL Server (DataDirect)

Налаштуйте джерело даних MS SQL Server DataDirect у вашій системі Guardium.

- MySQL

Налаштуйте джерело даних MySQL у вашій системі Guardium.

- Neo4j

Налаштуйте джерело даних Neo4j у вашій системі Guardium.

- Netezza

Налаштуйте джерело даних Netezza® у вашій системі Guardium.

- Oracle (Data Direct – Назва служби)

Налаштуйте джерело даних Oracle із підключенням DataDirect у вашій системі Guardium.

- Oracle (прямі дані - SID)

Налаштуйте джерело даних Oracle із підключенням DataDirect у вашій системі Guardium.

- PostgreSQL

Налаштуйте джерело даних PostgreSQL у вашій системі Guardium.

- SAP HANA

Налаштуйте джерело даних SAP HANA у вашій системі Guardium.

- SQL DB Azure

Налаштуйте джерело даних SQL DB Azure у вашій системі Guardium.

- Sybase

Налаштуйте джерело даних Sybase у вашій системі Guardium.

- Sybase IQ

Налаштуйте джерело даних Sybase IQ у вашій системі Guardium.

- ТЕРАДАТА

Налаштуйте джерело даних TERADATA у вашій системі Guardium.. [7]

Налаштування спеціальних властивостей для ваших джерел даних

Збільште свої джерела даних, визначаючи та призначаючи власні властивості.

Налаштувавши власні властивості, ви можете краще керувати своїми джерелами даних, організовувати ваш робочий процес і ефективно виконувати складні процеси.

Розглянемо сценарій, у якому ви хотіли б оцінити вразливість джерел даних у певному географічному місці. Ви можете визначити назву розташування як спеціальну властивість, призначте властивість усім джерелам даних, які знаходяться в ньому

Розташуйте та згрупуйте джерела даних за спеціальною властивістю. Спеціальна властивість може також бути додати до наявної групи джерел даних. Тепер можна налаштувати захист оцінки для сканування лише активних джерел даних, які є в групі.

Користувацькі властивості є гнучкими і за потреби їх можна змінити або видалити. Ти можеш створити будь-яку кількість індивідуальних властивостей на основі потреб вашого бізнесу та призначити кілька властивостей до одного джерела даних. Ви також можете імпортувати наявні значення з додатку для моніторингу відповідності Guardium®.

Обрано імпорт вручну

- Властивості або динамічно імпортувати оновлені значення, коли до них додаються нові властивості
- Моніторинг відповідності. Коли ви експортуєте джерело даних, призначені властивості також експортується.

Ви можете збагатити своє джерело даних двома простими кроками:

1. Визначте спеціальну властивість з одним або кількома пов’язаними значеннями.

2. Призначте налаштовану властивість своєму джерелу даних.

Наступна процедура детально описує процес налаштування.

Процедура

1. Відкрийте інструмент «Визначення джерела даних», натиснувши « Налаштування» > « Інструменти та». Перегляди > Визначення джерела даних .

2. Щоб додати нову користувацьку властивість, клацніть Спеціальні властивості > Керувати

a. У вікні Керування користувацькими властивостями клацніть, щоб створити а власність на замовлення. У полі Назва властивості введіть назву власність на замовлення. Приклад: центр обробки даних.

б. У розділі Дійсні значення клацніть, щоб додати одне або кілька користувацьких значень до власність на замовлення. Приклад: Нью-Йорк, Сан-Франциско, Чикаго.

c. Натисніть Зберегти .

d. Повторіть кроки2.a до2.c, щоб додати більше спеціальних властивостей на основі ваших потреби бізнесу. Приклади: Країна, Континент, Бізнес-одиниця. Ти можеш створити будь-яку кількість користувацьких властивостей з будь-якою кількістю пов’язаних цінності.

3. Щоб призначити спеціальну властивість, виберіть джерело даних або групу джерел даних Datasource визначення сторінки. Потім натисніть Користувацькі властивості > Додати до джерела даних .

a. Виберіть відповідну назву властивості зі спадного меню.

б. Виберіть відповідне значення зі спадного меню.

c. Натисніть +Додати інше, щоб додати іншу спеціальну властивість до джерело даних. Ви можете додати кілька властивостей до одного джерела даних або група джерел даних.

d. Натисніть Зберегти, щоб призначити властивості вибраному джерелу даних або групі.

4. Додатково: призначте додаткові властивості, повторивши крок 3. Ви також можете редагувати

джерело даних, вибравши джерело даних, потім натиснувши , перейшовшина вкладці Custom та вибравши інше значення для джерела даних.

5. Необов’язково. Якщо можливо, імпортуйте власні властивості з галузі та програми групи, які ви визначили під час моніторингу відповідності Guardium

додаток. Ви можете імпортувати всі або вибрані властивості. Установіть прапорець Update custom DataSource властивість з промисловістю і оновленням додатків для динамічно імпортувати властивості та під час їх оновлення.

6. Необов'язково: змініть або видаліть спеціальні властивості, якщо потрібно. Коли користувацька властивість видаляється, він також видаляється з усіх пов’язаних джерел даних і джерел даних групи.

7. Перегляньте всі призначені властивості для джерела даних у джерелі даних

Сторінка " Визначення " в стовпці " Спеціальний ".[8]

3.2. Організація захисту визначених об’єктів

Після того, як ви визначите бази даних і файлові системи, які містять конфіденційні дані, ви можете взяти кілька кроків для захисту цих даних. Варіанти захисту включають маскування даних, оповіщення персонал на основі доступу до даних та встановлення політики, що забезпечує доступ обмеження.

Аналітика активних загроз

На інформаційній панелі Active Threat Analytics відображаються потенційні випадки порушення безпеки на основі зовнішнього процесу видобутку та виявлені симптоми атаки. На цій панелі можна переглядати та розслідувати справи, а також вживати заходів щодо окремих випадків.

Спостерігач ризиків

Risk Spotter – це перша в своєму роді технологія, яка змінює парадигму безпеки на Політика захисту даних штучного інтелекту. Він використовує цілісний алгоритм, яким динамічно оцінює фактори ризику, а також використовує розумний алгоритм для визначення потенційних ризиків для всєї системи.

Виявлення викидів

Увімкніть і почніть аудит виявлення викидів у два простих кроки, дозволивши Guardium зробити цю роботу з виявлення ненормальної поведінки сервера і користувачів, а також забезпечення раннього виявлення можливих нападів.

Оцінювач довіри в режимі реального часу

Оцінювач довіри в режимі реального часу відстежує та оцінює ваш Guardium® S-TAP з’єднання, щоб позначити з’єднання як надійні чи ненадійні.

Налаштування активної аналітики загроз

Політика

Політики — це набори правил і дій, що застосовуються в реальному часі до спостережуваного трафіку бази даних за системою Guardium. Політики визначають, який трафік ігнорується чи реєструється, які дії вимагають більш детального ведення журналу, а також те, які дії повинні викликати сповіщення або блокувати доступ до бази даних.

Сповіщення про кореляцію

Сповіщення – це повідомлення, яке вказує на те, що було виявлено виняток або порушення правил політики. Як позначати події за допомогою сповіщень про кореляцію Можна активувати сповіщення про кореляцію, якщо в останніх трьох є більше п’ятнадцяти помилок SQL годин від будь-якого окремого користувача програми.

Управління інцидентами

Додаток інтегрованого управління інцидентами (IIM) забезпечує бізнес-користувача інтерфейсом з автоматизацією робочого процесу для відстеження та вирішення проблем безпеки бази даних інциденти.

Управління інцидентами - відстежуйте та вирішуйте інциденти безпеки бази даних.

Перепис запиту

Функція перезапису запитів забезпечує детальний контроль доступу до баз даних, перехоплення запитів до бази даних і їх перезапис на основі критеріїв, визначених у безпеці політики.

Політики файлової активності для файлових серверів UNIX і Windows

Політики діяльності з файлами використовуються для захисту конфіденційних даних на файлових серверах UNIX, Windows.

Політики діяльності з файлами для мережевого сховища (NAS) і SharePoint

Налаштуйте моніторинг активності файлів для пристроїв NAS і SharePoint, визначивши політики та правила в Конструкторі політик для файлів.

Налаштування консолідації подій FAM MS Office

Використовуйте функцію консолідації подій Office FAM монітора, щоб відфільтрувати сторонні, невідповідні дії з файлами MS Word, Excel та PowerPoint. [9]

Active Threat Analytics

На інформаційній панелі Active Threat Analytics відображаються потенційні випадки порушення безпеки на основі зовнішнього процесу видобутку та виявлені симптомів атаки. На цій панелі можна переглядати та розслідувати справи, а також вживати заходів щодо окремих випадків. Active Threat Analytics працює на центральних менеджерах і автономних підрозділах. Необхідна умова: увімкнено пошук загроз і видобуток DAM Outlier. Натисніть Активне Посилання на налаштування аналітики загроз, щоб увімкнути пошук загроз і видобуток DAM Outlier. Активний Аналітика загроз показує результати для всіх колекторів, на яких здійснюється видобуток DAM Outliery вімкнено. Отримайте доступ до Active Threat Analytics зі сторінки привітання або виберіть Захист > Розкрити вектори загроз > Active Threat Analytics. У верхньому рядку результатів зведено

основні випадки та відкриті випадки для: баз даних, користувачів БД або користувачі ОС, файлові системи та користувач файлів. Випадки в кожній категорії визначаються за своїми рівнями ризику: високий, середній і низький. Якщо користувач бази даних/файлової системи/ОС є користувачем пов’язані з кількома випадками, ця база даних або користувач враховується лише один раз.

Наприклад, існує 40 основних випадків, 10 з яких пов’язані з базою даних NN, а 10 з них пов'язані з користувачем XX, а інші 20 пов'язані з різними базами даних/користувачами. Загальна кількість випадків баз даних і файлових серверів, буде 22, а не 40. За замовчуванням дані відображаються за останній день. Ви можете змінити період часу з випадаючого списку. На графіку показано порушення, відхилення, помилки та дії за той самий період часу. У таблиці наведено всі основні випадки (у порядку спадання тяжкості), включаючи тип загрози, спостережувану діяльність, на якій ґрунтується справа, та деталі джерела. Активний Threat Analytics визначає потенційні порушення безпеки за типом справи, переліченим у Загроза.

Натисніть Бази даних , користувач БД , файли системи і користувач ОС , щоб відкрити резюме з суб'єктів з відкритими справами. Звідти ви можете натиснути «Переглянути профіль», щоб відкрити «Поведінковий». Аналіз для конкретної бази даних або користувача та перегляд усіх випадків, пов’язаних із цим об’єктом, розподіл робочого часу та розподіл дієслів. Для користувачів бази даних ви також можете натиснути «Індикатори ризику користувача», щоб відкрити вікно «Відомості про ризик», у якому буде показано ризик.

Оцінки індикатора ризику Spotter.

Кожен випадок високого ступеня тяжкості є підозрюваною загрозою, яку слід розслідувати негайно. Важкі випадки також можуть бути викликані встановленням виправлення. У цьому справу, ви б закрили справу. Випадки низької тяжкості можуть бути аномаліями. Якщо так, подумайте про закриття справи.

При розслідуванні справ:

- Отримайте чітку картину, чи це одиничний випадок, чи один із багатьох джерел.

- Змініть таймфрейм або фільтри на вужчий або ширший перетин і подивіться для моделей або іншої незвичайної поведінки.
- Подивіться на розподіл діяльності, розподіл у часі, середнє значення діяльність, помилки тощо.
- Для користувачів бази даних подивіться на оцінку ризику та аналіз.

Таблиця випадків

- Натисніть поруч з номером справи , щоб відкрити сторінку Case Analysis , даючи детальний аналіз справи з кількох точок зору. Це вихідна точка ваше розслідування:
- Інформація про джерело: статистика та діяльність щодо джерела, поширення діяльності за періодом часу, історією справ і типами, які були відкриті (ізакрито) на цьому джерелі.
- Деталі справи: час, тип, спостереження, деталі, специфічні для типу справи, і посилання на повний звіт SQL. Період часу за замовчуванням для повногоЗвіт SQL становить одну годину. Розслідуючи справи, дивіться також на менший час періоди та більш ранні періоди часу.
- Дослідження: п'ять наборів графіків, які дають контекст для цього випадку та забезпечують глибоке занурення у ваше розслідування.Де: Додаткова інформація про сервер і базу даних, наприклад, кількість баз даних (та їх типів) на сервері, кількість випадків того ж типу, що можна побачити в базі даних. Коли: Деталі періоду часу: робочі години, позаробочий час, вихідні, що ще трапилося за цей час. Що: деталі подібних випадків: статистика випадків, чутливі об'єкти доступ (і за допомогою яких команд), інші випадки цього випадку(і де).Хто: Статистика користувачів, які отримали доступ до бази даних, користувачів, які зазвичай отримують доступ до цієї бази даних (користувачі ОС, користувачі БД) і з якого клієнтського хоста. Для користувачів ОС: клієнт розміщує доступ до цього користувача, і коли він був вперше використаний (як записано в Guardium). Як: Статистика програм, які використовуються для доступу до бази даних. Програми, які використовувалися протягом періоду часу, програми, які зазвичай використовуються, Перший запис про використання програми(як записано в Guardium).Ви також можете вжити заходів щодо окремих випадків:

- Призначити випадок: призначте справу ролі, електронній пошті, групі користувачів або користувачу.
- Переважні ролі та групи, оскільки це можуть робити окремі користувачі та електронні листимінити.
- Додати до групи: Виберіть одне з: IP-адреса сервера, база даних, користувач БД, файлова система, файл користувача та додайте його до наявної або нової групи. Це корисно для відстеження користувачів і активності. Ви можете використовувати ці групи в політиках, звіти, сповіщення для покращеного моніторингу вашої системи.
- Закрити регістр: якщо спостережувана поведінка прийнятна, розгляньте можливість закриття випадок.
- Додайте коментар.
- Відфільтруйте всю таблицю за категорією загроз за допомогою спадного меню, відфільтруйте за допомогою поле вільного тексту, і ви можете вживати заходів щодо окремих випадків. Ці дії меню має ті самі параметри, що й меню регістра, з одним доповненням: Відкрити панель керування справами: відкриває панель інструментів розслідування, відфільтровану за обраний випадок. Детальніше про симптоми, порівняйте з іншими БД і користувачів, а також переглядати активність за певний час. Подивитися Панель інструментів розслідування
- Випадки загроз не копіюються до додаткового центрального менеджера. У разі відмовлення, немає відомих випадків загроз у новому первинному центральному менеджері. [10]

Risk Spotter functions

Дізнайтеся, як Risk Spotter визначає ризикованих користувачів у всій вашій системі. Risk Spotter працює на центральних менеджерах і в автономних системах. Усі колекціонери повинні працювати під керуванням V11.0 або новішої.

Risk Spotter реалізує динамічну оцінку ризику, враховуючи численні ризики фактори, у тому числі:

- Уразливості та порушення, пов’язані з користувачем;
- Помилки;

- Результати аналізу загроз;
- Діяльність у неробочий час (визначається як after hours робота та перед годинами роботи на сторінці Конструктора періодів часу та розподіляється від центрального менеджера до його керованих підрозділів.);
- Обсяг доступу до даних;
- Обсяг діяльності;
- Доступ до конфіденційних даних;
- Тип команд, які виконував користувач (DML, DDL, SYSTEM і так далі).

Алгоритм Risk Spotter використовує модулі Guardium для аналізу індикаторів ризику та для виявлення ризикованих користувачів. Загальний рейтинг ризику кожного користувача розраховується щодня на основі перевірених даних. Risk Spotter призначає кожному користувачеві оцінку в діапазоні від 0 до 10. Детальні дані про ризики представлені в таблиці Risky Users на сторінці Risk Spotter. Щоб максимізувати переваги Risk Spotter, запровадьте власну Risk Spotter Dynamic

Політика аудиту, яка використовує групу Контролер ризиків – перевірені ризиковані користувачі. Коли ви запровадити політику динамічного аудиту:

Guardium® додає три типи користувачів до Risk Spotter – перевірені ризиковані користувачі групі та постійно перевіряє групу. Є три типи користувачів:

- Найбільш ризиковані користувачі: користувачі, визначені разом за алгоритмом Risk Spotter з вашими встановленими політиками. Користувачі цієї групи переносяться, якщо їх оцінка ризику виправдовує це. (Список найбільш ризикованих користувачів не копіюється до середнього центрального менеджера. У разі відмовлення, Топ ризиковано список користувачів порожній у новому первинному центральному менеджері.)
- Користувачі зі списку спостереження: Список спостереження – це група користувачів, для яких ви заповнюєте подальше спостереження або розслідування. Ви можете додати будь-якого користувача до списку спостереження. Ці користувачі залишаються в групі «Список спостереження» в

наступних щоденних звітах про ризики ітерації, незалежно від їхньої оцінки ризику.

- Користувачі з випадковою вибіркою: Risk Spotter безперервно сканує вашу систему, за межами вашої політики, оцінювання незареєстрованих користувачів і виявлення потенційних ризикованих користувачів.

Risk Spotter– аудит членів групи ризикованих користувачів і повторно встановлює політику під час щоденного процесу (1:00-2:00), ефективно оновлюючи будь-яку політику, яка його використовує.

Guardium постійно контролює ресурси. Якщо ресурси керованого підрозділу є перевантаженими з будь-якої причини, Guardium автоматично видаляє динамічну політику аудиту для перевантажених керованих одиниць. Видалення політики не впливати на членів групи Ризик-спостерігач – перевірені ризиковані користувачі або Ризик Spotter - група спостережень. Користувач, якого перевіряє лише динамічний аудит політики не перевіряється в день видалення політики. Нові ризиковані користувачі, у яких не встановлено політику, не додаються до Risk Spotter – Група ризикованих користувачів перевірена, а оцінка ризику наявних користувачів не оновлюється. Натисніть Журнали та стан, щоб відкрити журнал подій Risk Spotter, щоб побачити, які керовані блоки не мають встановленої політики. [11]

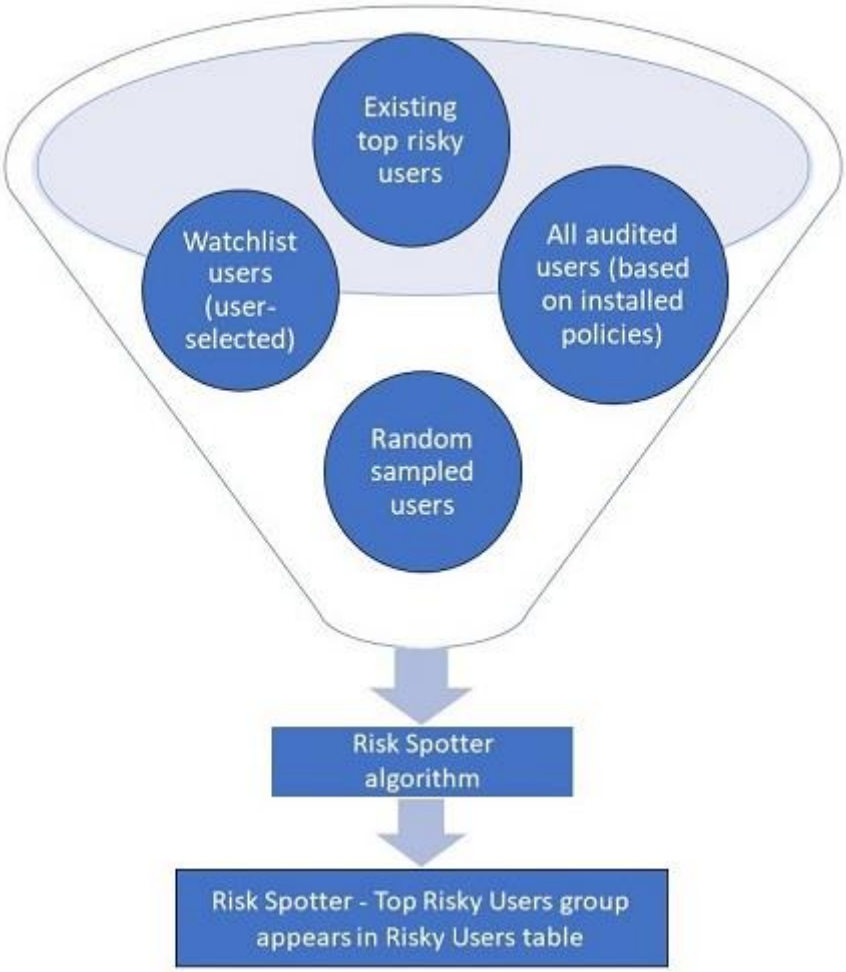

Рис. 3.4. Наповнення групи найбільш ризикованих користувачів

3.3. Розроблення рекомендацій щодо забезпечення захищеності інформаційних об’єктів ресурсами IBM GUARDIUM

У попередніх розділах було визначено причини та необхідність захисту інформації у корпоративних системах, а також детально розглянуто можливості технології IBM GUARDIUM. На основі цього сформовано перелік рекомендацій щодо організації безпеки:

1. Обрати рішення IBM GUARDIUM, зо задовільнить потреби компанії
2. Зробити базові налаштування інтерфейсу в залежності від поставлених завдань та приіоритетних напрямів
3. Провести ідентифікацію джерел даних з якими повинен взаємодіяти IBM GUARDIUM, за потреби провести кастомізацію джерел
4. Обрати методи та технології захисту, що необхідні компанії з числа:

- активне виявлення атак
- системи ідентифікації ризиків
- Виявлення викидів
- Оцінювач довіри в режимі реального часу
- Активна аналітика загроз
- Політика
- Сповіщення про кореляцію
- Управління інцидентами
- Перепис запитів
- Політики файлової активності для файлових серверів UNIX і Windows
- Політики діяльності з файлами для мережевого сховища (NAS) і SharePoint
- Налаштування консолідації подій FAM MS Office

5. Провести налаштування систем аудиту та моніторингу вікористовуючі необхідні інструменти з перелику:

- Основна політика моніторингу безпеки даних
- Розумний помічник для моніторингу відповідності
- Панель інструментів розслідування
- Аналітика виявлення загроз
- Панель захисту даних
- Побудова процесів аудиту
- Зовнішня кореляція даних
- Набори конфіденційності
- Спеціальне сповіщення
- Процес журналу
- Запуск звітів про права на базу даних
- Ідентифікація користувача
- Аудит зміни вартості
- Створення бази даних аудиту
- Контроль доступу до таблиці

- Встановлення та активація FamMonitor на серверах Windows
- Монітор активності файлів для NAS і SharePoint
- PCI/DSS Accelerator для забезпечення відповідності PCI
- Конструктор робочих процесів

6. Організувати автоматичну генерацію звітів безпеки використовуючи інструменти:

- Попередньо визначені звіти
- Створення інформаційних панелей та додавання звітів
- Відкриття інформаційної панелі дослідження, відфільтровано для об’єктів звіту
- Використання конструктора запитів-звітів
- Домени, сутності та атрибути
- Користувацькі домени
- KData Mart
- Конструктор розподілених звітів
- Робота з викликами та звітами API
- Робота із зовнішніми каналами
- Створення звітів для z/OS

На цьому етапі базові рекомендації закінчуються, у разі потреби більш широкого функціоналу необхідно розглядати над будові до системи IBM GUARDIUM, що надають можливість розширити функціонал та підвищиті рівень захищеності системи. Наприклад можна скористатися надбудовою Guardium® Vulnerability Assessment, де можна створити сканування оцінки безпеки та аудит робочого процесу, щоб автоматично виявляти та виявляти вразливості бази даних, активно покращуючи конфігурації та посилюючи інфраструктуру.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення захисту корпоративної інформаційної системи, встановлена сутність завдань їх захисту. Встановлено сутність та зміст управління захистом корпоративної інформаційної системи.

Проаналізовано існуючі технології управління захистом корпоративної інформаційної системи. Досліджена технологія управління захистом корпоративної інформаційної системи на базі платформи IBM GUARDIUM.

Визначено методи та засоби забезпечення управління даними, що циркулюють у корпоративній інформаційній системі, які реалізовані в IBM GUARDIUM.

Встановлено основні функції та принципи роботи платформи IBM GUARDIUM Платформа IBM GUARDIUM – програмне забезпечення, що забезпечує швидке та інтуїтивно зрозуміле рішення для управління корпоративнім інформаційним середовищем і його безпекою та дозволяє організаціям бачити і управляти фізичними і віртуальними наборами даних за допомогою єдиної інфраструктури.

Досліджено типову архітектуру рішення IBM GUARDIUM, яка надає уявлення про середовище платформи та можливість її правильного планування застосування.

У роботі запропоновано варіант технології управління захистом корпоративної інформаційної системи на платформі IBM GUARDIUM. для цього було розглянуто основні процеси направлені на захист інформаційних ресурсів корпоративного середовища, що запропоновані у IBM GUARDIUM

Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління захистом корпоративної інформаційної системи на підприємстві на основі базового функціоналу системи.

Таким чином, правильна реалізація технології управління захистом корпоративної інформаційної системи на платформі IBM GUARDIUM має

забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Фролов Е.Б. Современные концепции управления в производственной логистике, MES для дискретного производства — метод вычисляемых приоритетов // САПР и графика : журнал. — М. : Компьютер Пресс, 2011. — № 1. — С. 71-75. — ISSN 1560-4640.
2. Інформаційна безпека [Електронний ресурс] // smart-soft. – 2019. – Режим доступу до ресурсу: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/.
3. Штучний інтелект у ІБ [Електронний ресурс] // sciencedirect. – 2020. – Режим доступу до ресурсу https://www.sciencedirect.com/science/article/pii/S2352484721007289
4. Огляд Гардіум [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=overview-guardium
5. Гартнер топ-10 [Електронний ресурс] // gartner. – 2020. – Режим доступу до ресурсу https://www.gartner.com/smarterwithgartner/gartners-top-10-technologies-for-information-security
6. Пошук джерел [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=discover
7. Джерела даних [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=datasources-creating-datasource-definition
8. Персоналізація джерел даних [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=datasources-configuring-custom-properties-your
9. Огляд систем захисту [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=protect

10. Активний аналіз загроз [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=protect-active-threat-analytics
11. Виявлення ризиків [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=spotter-risk-functions
12. Аудит та моніторинг [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=monitor-audit
13. 13 Адміністрування [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=system-guardium-administration
14. 14 Сповіщення [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=alerts-notifications
15. Розвиваючись технології захисту інформації [Електронний ресурс] // techbeacon. – 2021. – Режим доступу до ресурсу: https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield
16. Встановлення регістраційних блоків[Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=installation-registering-units
17. Центральний менеджмент [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=central-management
18. Компоненти та сервіси менеджменту [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/guardium/11.4?topic=management-guardium-component-services
19. Імплементація центрального менеджменту у новій інсталяції [Електронний ресурс] // IBM. – 2021. – Режим доступу до ресурсу:

https://www.ibm.com/docs/en/guardium/11.4?topic=management-implementing-central-in-new-installation

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)