НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінка ефективності рішень керування доступом у хмарній інфраструктурі для впровадження організаціями політики Zero Trust

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-01

Новак Ольга Ігорівна _____
(підпис)

Керівник к.т.н., доцент, доцент кафедри Інформаційної безпеки

Гальчинський Леонід Юрійович _____
(підпис)

Рецензент _____. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі
запозичень з праць інших
авторів без відповідних посилань
Здобувач вищої освіти _____
(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Новак Ольга Ігорівна

1. Тема роботи «Оцінка ефективності рішень керування доступом у хмарній інфраструктурі для впровадження організаціями політики Zero Trust», керівник роботи к.т.н., доцент, доцент кафедри Інформаційної безпеки Гальчинський Леонід Юрійович

затверджені наказом по університету від « » _____ 2024 р. №

2. Термін подання здобувачем вищої освіти роботи 11 червня 2024 р.

3. Вихідні дані до роботи: статті про можливе застосування принципів Zero Trust в Amazon AWS та офіційна документація виробника CIEM рішення Tenable Cloud Security

4. Зміст роботи: огляд принципів політики безпеки Zero Trust, їх впровадження в хмару за допомогою сервісів Amazon AWS та CIEM рішень, огляд та використання методу аналітичних мереж для оцінки ефективності CIEM рішень, розробка методичних рекомендацій для впровадження організаціями політики Zero Trust

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) презентація

6. Дата видачі завдання 05 грудня 2023 р.

Календарний план

No з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вибір теми роботи, формування завдання та мети	01.12.2023-20.12.2023	виконано
2	Опрацювання літературних джерел	20.12.2023 - 16.03.2024	виконано
3	Ознайомлення з базовим функціоналом сервісів Amazon AWS для впровадження Zero Trust	17.01.2024-01.04.2024	виконано
4	Ознайомлення з класом рішень CIEM та його принципами роботи на прикладі Tenable Cloud Security	02.04.2024-20.04.2024	виконано
5	Ознайомлення з методами оцінки ефективності роботи на основі багатокритеріального вибору та визначення критеріїв	21.04.2024-05.05.2024	виконано
6	Проходження переддипломної практики	15.04.2024-19.05.2024	виконано
7	Аналіз отриманих результатів експертного оцінювання та обрахунок фінальної оцінки ефективності	06.05.2024-20.05.2024	виконано
8	Розробка методичних рекомендацій	21.05.2024-28.05.2024	виконано
8	Оформлення дипломної роботи	28.05.2024-05.06.2024	виконано
9	Передзахист дипломної роботи	11.06.2024	виконано
10	Захист дипломної роботи	18.06.2024	виконано

Здобувач вищої освіти _____ Ольга НОВАК
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

Керівник роботи _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Дипломна робота містить: 58 сторінок, 19 ілюстрацій, 14 таблиць, 1 додаток, 25 джерел літератури.

Метою роботи є аналіз функціоналу рішень контролю доступу у хмарі, їх співставлення з принципами політики Zero Trust, дослідження методів оцінки багатокритеріального аналізу та оцінка ефективності рішень контролю доступу у хмарі для впровадження організаціями політики Zero Trust.

Об’єктом дослідження є рішення контролю доступу у хмарі Tenable Cloud Security та сервіси хмарного провайдера Amazon AWS.

Предметом дослідження є оцінювання ефективності рішень контролю доступу у хмарі для організаціями впровадження політики Zero Trust, що має на меті мінімізацію кіберзагроз з боку шкідливих маніпуляцій користувачів з хмарними ресурсами.

Методами дослідження є аналіз літературних джерел за обраною тематикою, дослідження та аналіз функціоналу рішень контролю доступу у хмарі, вибір методу багатокритеріального аналізу для оцінки ефективності рішень контролю доступу у хмарі експертами , розробка методичних рекомендацій, спрямованих на покращення безпеки хмарних середовищ та гнучкого впровадження політики Zero Trust.

Робота містить опис принципів політик Zero Trust, їх використання у сервісах хмарного провайдера Amazon AWS, аналіз функціоналу рішень контролю доступу у хмарі на прикладі Tenable Cloud Security, методів багатокритеріального аналізу. Використано один з методів для оцінки ефективності рішень контролю доступу у хмарі для впровадження політики Zero Trust та розроблено методичні для покращення роботи з ними.

Ключові слова: контроль доступу у хмарі, надлишкові права, оцінка ефективності, Zero Trust, метод аналітичних мереж.

ABSTRACT

Thesis contains: 58 pages, 19 illustrations, 14 tables, 1 appendix, 25 sources of literature.

The purpose of the study is to analyse the functionality of cloud access control solutions, compare them with the principles of the Zero Trust policy, study methods for evaluating multi-criteria analysis and assess the effectiveness of cloud access control solutions for implementing the Zero Trust policy by organisations.

The object of the study is the Tenable Cloud Security cloud access control solution and the services of the Amazon AWS cloud provider.

The subject of the study is to evaluate the effectiveness of cloud access control solutions for organisations implementing the Zero Trust policy, which aims to minimise cyber threats from malicious user manipulation of cloud resources.

The research methods include analysis of literature on the selected topic, research and analysis of the functionality of cloud access control solutions, selection of a multi-criteria analysis method for assessing the effectiveness of cloud access control solutions by experts, development of methodological recommendations aimed at improving the security of cloud environments and flexible implementation of the Zero Trust policy.

The paper describes the principles of Zero Trust policies, their use in the services of the Amazon AWS cloud provider, analyses the functionality of access control solutions in the cloud on the example of Tenable Cloud Security, and methods of multicriteria analysis. One of the methods for evaluating the effectiveness of access control solutions in the cloud for implementing the Zero Trust policy is used and methodological methods for improving the work with them are developed.

Keywords: access control in the cloud, excessive rights, efficiency assessment, Zero Trust, analytical network method.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПХП – Постачальник Хмарних Послуг

CIEM – Системи керування контролю доступом (англ. Cloud Infrastructure Entitlement Management)

BYOD – Концепція бери свій власний девайс (англ. Bring-Your-Own-Device)

JiT – Надання доступу у цей час (англ. Just-in-Time)

MCDA – Багатокритеріальний аналіз (англ. Multi-Criteria Decision Analysis)

TOPSIS – Метод для визначення переваги за схожістю до ідеального рішення (англ. Technique for Order Preference by Similarity to Ideal Solution)

AHP - метод аналізу ієрархій (англ. Analytic Hierarchy Process)

ANP – метод аналітичних мереж (англ. Analytic Network Process)

Хмарне навантаження - логічний набір програмного забезпечення та даних, які присутні в хмарі і обробляються за допомогою технології хмарних обчислень

ВСТУП

Актуальність роботи зумовлена вимушеною міграцією організацій на використання хмарних сервісів та відповідне збільшення проблем безпеки зберігання чутливих даних та ресурсів у хмарних середовищах. Розроблена для такого політика Zero Trust вимагає дотримання певних принципів, які досить складно регулювати в умовах масштабування і відповідно був створений окремий клас рішень з кібербезпеки – CIEM. Незважаючи на його можливості постає питання ефективності використання такого роду систем для гнучкого впровадження політик Zero Trust у хмари організацій.

Метою роботи є аналіз функціоналу рішень контролю доступу у хмарі, їх співставлення з принципами політики Zero Trust, дослідження методів оцінки багатокритеріального аналізу та оцінка ефективності рішень контролю доступу у хмарі для впровадження організаціями політики Zero Trust.

Об’єктом дослідження є рішення контролю доступу у хмарі Tenable Cloud Security та сервіси хмарного провайдера Amazon AWS.

Предметом дослідження є оцінювання ефективності рішень контролю доступу у хмарі для організаціями впровадження політики Zero Trust, що має на меті мінімізацію кіберзагроз з боку шкідливих маніпуляцій користувачів з хмарними ресурсами.

Для досягнення мети дослідження, було сформовано наступні **завдання**:

1. Проаналізувати принципи політики Zero Trust та їх використання у сервісах хмарного провайдера Amazon AWS;
2. Провести аналіз функціоналу рішень контролю доступу у хмарі на прикладі Tenable Cloud Security та визначити критерії оцінювання їх ефективності;
3. Дослідити методи багатокритеріального аналізу та обрати найкращий для оцінки експертами;
4. Розробити методичні рекомендації для покращення роботи з рішеннями контролю доступу у хмарній інфраструктурі на основі отриманих результатів.

Методами дослідження є аналіз літературних джерел за обраною тематикою, дослідження та аналіз функціоналу рішень контролю доступу у хмарі, вибір методу багатокритеріального аналізу для оцінки ефективності рішень контролю доступу у хмарі експертами , розробка методичних рекомендацій, спрямованих на покращення безпеки хмарних середовищ та гнучкого впровадження політики Zero Trust.

Практичне значення одержаних результатів полягає у розробці рекомендацій для організацій щодо підвищення ефективності вибору та впровадження рішень контролю доступу у хмарній інфраструктурі відповідно до принципів політики Zero Trust. Це дозволить покращити захист даних і ресурсів у хмарних середовищах та зменшити ризики кіберзагроз.

1 ОГЛЯД ВИКОРИСТАННЯ ХМАРНИХ РЕСУРСІВ У IT-СЕКТОРІ. РЕГУЛЮВАННЯ ПРИНЦИПІВ ZERO TRUST У ХМАРІ

Сьогодні поняття «хмара» та «хмарні технології» стали дуже розповсюдженими у світі IT, адже з їх використанням неабияк підвищились ефективність та швидкість обробки даних, що вплинуло на розвиток розробки програмного забезпечення, штучного інтелекту та й навіть на гнучку експлуатацію IoT(Internet of Things) девайсів. [1] Хмарні технології – це модель роботи, за допомогою якої компанія отримує доступ до загальних обчислювальних ресурсів на кшталт серверів, сховищ, мережі, додатків та інших хмарних послуг.

За даними Forbes станом на 2024 рік вже йдеться мова про мультихмарну чи гібридну еволюцію, яка в свою чергу надасть кожній організації можливість гнучко поєднувати всі свої сервіси та обчислювальні потужності в одному просторі. За цим стоятиме:

- Поєднання приватної та публічної хмари;
- Розповсюдження безсерверних архітектур;
- Популяризація контейнерних оркестраторів;
- Використання штучного інтелекту та машинного навчання для оптимізації ресурсів. [2]

На рисунку 1.1 зображено схему доступу до приватної хмари у хмарному провайдері Amazon AWS, як приклад поєднання хмари та наземного інфраструктур.

А в дослідженнях Gartner очікується великий попит на використання хмарних ресурсів користувачами, а саме збільшення ринкової частки на 20,4%.Усі сервіси в хмарі очікують зростання, а саме у таблиці 1 відображено прогнозовану різницю у інвестиціях порівняно з 2023 роком.

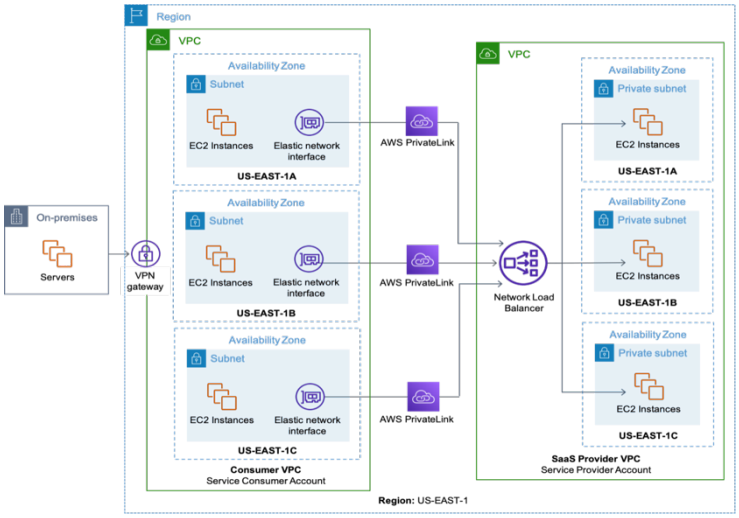

Рисунок 1.1 – Схема доступу до хмарних сервісів AWS [3]

Таблиця 1.1 - Прогноз витрат користувачів публічних хмарних сервісів у світі (у мільйонах доларів США) [4]

	2023	2024	Зріст у %
Платформа як сервіс (PaaS)	145,320	176,493	21,5%
Інфраструктура як сервіс (IaaS)	143,927	182,222	26,6%
Програмне забезпечення як сервіс (SaaS)	205,221	243,991	18,9%
Бізнес-процес як сервіс (BPaaS)	66,339	72,923	9,9%
Робоче місце як сервіс (DaaS)	2,784	3,161	13,5%

Такий попит пояснюється декількома факторами, які включають не лише обмеженість організацій у власних обчислювальних чи фінансових ресурсах, але і необхідність у віддаленому доступі до певних об'єктів без географічної прив'язки. Крім того, зростаюча потреба у масштабній цифровізації змушує компанії шукати ефективні та гнучкі рішення для зберігання, обробки та аналізу даних, що доволі часто вимагає використання хмарних ресурсів. [5]

Українські компанії у зв’язку з повномасштабним вторгненням були вимушені евакуювати своїх співробітників зі сходу та півдня країни до інших областей, а також організувати робочі процеси віддалено, для чого й необхідні хмарні сервіси. До того ж, дуже гостро стоїть проблема безпеки фізичної

інфраструктури та даних, адже внаслідок ракетних ударів вся серверна частина може бути знищена вщент, де жодні резервні копії не допоможуть, якщо вони були збережені лише локально.

Відповідно останні два роки відбувається поступова міграція на хмарні сервіси і організації власноруч обирають стратегії:

- Переміщення(«Lift and shift»)
- Реплатформинг(«Replatforming»)
- Повторна купівля(«Repurchasing»)
- Перебудова(«Refactoring»)
- Видалення(«Retiring»)
- Утримання(«Retaining»)

Розглянемо більш детально кожну з цих стратегій:

Переміщення(«Lift and shift»)

Як випливає з назви, це означає переміщення точної копії поточного (наземного) середовища без внесення значних змін до хмари для швидкої окупності інвестицій.

Реплатформинг(«Replatforming»)

Реплатформинг слугує варіацією переміщення, адже до поточного середовища передбачається внесення деяких додаткових змін для його оптимізації і ефективного використання у хмарі.

Повторна купівля(«Repurchasing»)

Дана стратегія передбачає перенесення лише певних додатків чи сервісів на новий, хмарний продукт, здебільшого на SaaS платформу.

Перебудова(«Refactoring»)

Це означає перебудову додатків з нуля, що зазвичай пов’язане з потребою використовувати хмарні можливості, які недоступні в існуючому середовищі, як-от безсерверні обчислення.

Видалення(«Retiring»)

За своєю назвою стратегія означає виявлення додатків в існуючому

середовищі, що більше не потрібні, і їх видалення задля ще більш заощадливого переміщення у хмару.

Утримання(«Retaining»)

Стратегія передбачає утримання від повної міграції у хмару, а розглядає лише переміщення тих критичних активів чи даних, що важливі для бізнесу. [6]

Дійсно, більшість компаній ще не зовсім готові до такої міграції, адже, за результатами опитування ISC2 43% користувачів мають певні сумніви стосовно рівня захищеності хмари. [7]

Так як міграція це завжди поступовий і довготривалий процес, зовнішня поверхня атаки організації стає все більшою і відповідно виникають потенційні загрози безпеки даних. Це може стати приводом для проведення кібератак на організацію, що може призвести до витоку конфіденційної інформації, втрати даних чи знищення інших ресурсів.

У зв'язку з цим організації повинні ретельно планувати та виконувати стратегії безпеки, включаючи шифрування даних, контроль доступу, моніторинг захисних систем та регулярні аудити безпеки. Проте одним з залізних аргументів використання хмарних ресурсів вважається підвищений рівень безпеки всіх даних відповідно до міжнародних стандартів. Однак на рисунку 1.2 відображається не зовсім задовільна статистика по шифруванню даних відносно до їх зберігання у хмарі.

Причиною цьому може слугувати недостатня обізнаність про роботу хмарних платформ або ж нехтування налаштуваннями безпеки, що надаються ПХП.

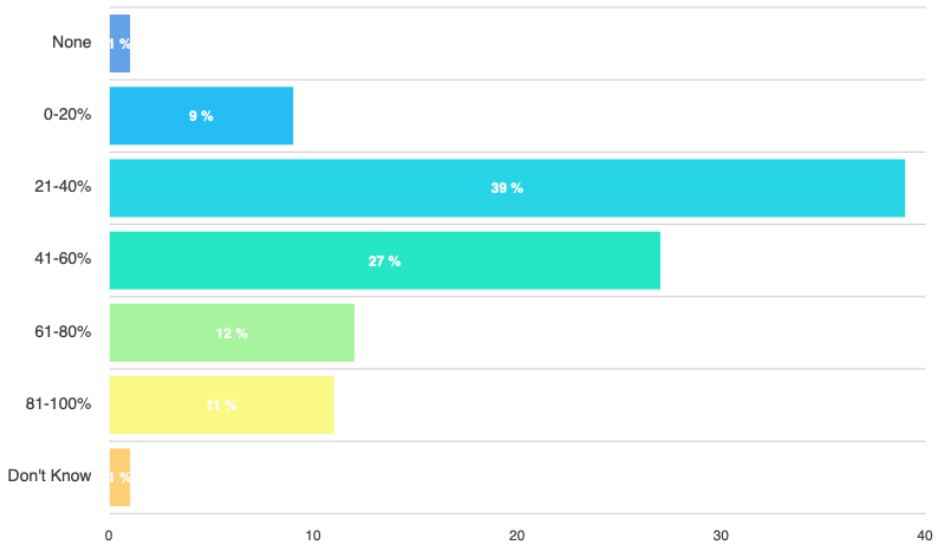

Рисунок 1.2 - Відсоток організацій, що шифрують чутливі дані у хмарі [8]

Даний факт підтверджується статистикою від ISC2 про рівень ознайомленості з хмарними платформами, що відображена на рисунку 1.3. Можна побачити, що лише четверта частина організацій достатньо розуміє, що таке хмара і як в ній працювати.

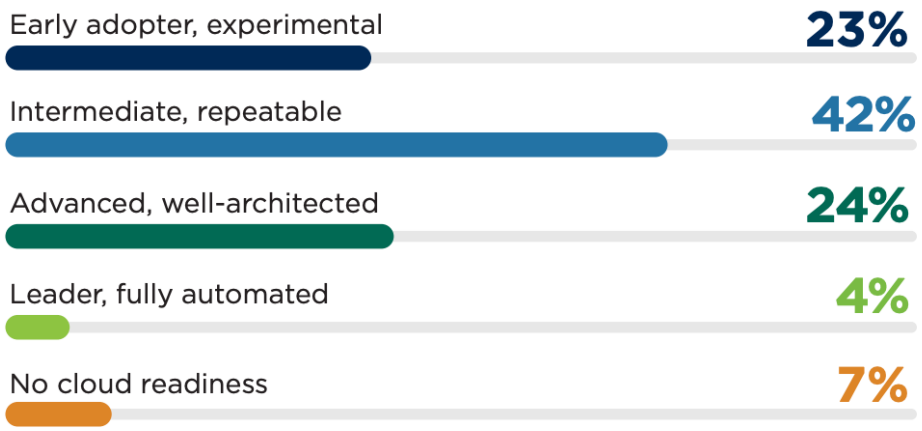

Рисунок 1.3 - Опитування стосовно рівня ознайомленості по роботі з хмарними середовищами [7]

Внаслідок такої недостатньої експертизи компанії та користувачі досі потерпають від кібератак та за дослідженням Thales за 2023 рік 55% всіх

інцидентів та витоків даних з хмари виникли через людську помилку, коли як експлуатація вразливостей містила лише 21%. [9]

1.1 Ризики та кібератаки на хмарні середовища

Хакерські атаки на хмарні сервіси можуть завдавати неабияких фінансових збитків, порушувати бізнес-процеси, шкодити репутації бренду та спричиняти витоки конфіденційної інформації. Тому важливо розуміти ризики безпеки та загрози, пов’язані з існуючою хмарною інфраструктурою, незалежно від того, чи це публічна хмара, приватна хмара, гібридна хмара чи будь-який інший тип.

Зрештою, раннє розуміння загальних ризиків допомагає побудувати надійну політику безпеки та дає можливість краще підготуватись до реагування на інциденти.

За даними британського університету York найголовнішими ризиками хмарних середовищ є:

1. Недостатня видимість поверхні атаки;
2. Неправильні конфігурації політик безпеки;
3. Порушення цілісності даних, їх витік;
4. Людські помилки; [10]

Однак даний список варто доповнити і такими традиційними для інформаційних систем ризиками, як:

5. Шкідливе програмне забезпечення;
6. Викрадення облікових записів;
7. Інсайдерські атаки. [11]

Розглянемо кожен з цих ризиків.

1. Недостатня видимість поверхні атаки

Вимушений чи добровільний перехід до хмарних технологій та популяризація віддаленої роботи внаслідок пандемії коронавірусу 2020 року і

військової агресії проти України призвели до величезної фрагментації поверхні атаки, що створює суттєву кількість «сліпих» зон, а відповідно полегшує зловмисникам пошук некерованих та вразливих активів. Кожне нове хмарне навантаження, яке підключається до хмарної платформи, створює абсолютно нову, нерегульовану поверхню атаки.

2. Неправильні конфігурації політик безпеки

Такі ПХП, як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud та IBM Cloud, є дуже розгалуженими і, внаслідок популяризації гібридних хмар або мультихмарної інфраструктури, багато організацій вирішують використовувати декілька з них. Це може породжувати певні ризики, оскільки у кожного ПХП вбудовані різні конфігурації та політики безпеки,які варто налаштовувати для стабільної роботи з хмарними ресурсами. Проігнорувавши даний важливий крок, можна створити купу критичних вразливостей та опорних точок атаки, якими скористаються кіберзлочинці.

3. Порушення цілісності даних, їх витік

Нікому не секрет, що дані – це основна ціль кібератак. І однією з причин початку використання хмари є саме захист даних та активів: багато підприємців занадто довіряють хмарі, що означає відсутність належного планування та відновлювальних ресурсів. Проте не існує повноцінного страхування від їх втрати, що може призвести і до ряду репутаційних збитків, фінансових втрат та затримку бізнесу.

4. Людські помилки

Людська помилка у контексті хмарних ресурсів несе ледь не найбільший ризик при розробці додатків чи банального регулювання доступу до певних обчислювальних ресурсів. Так, за оцінками Gartner, до 2025 року нестача обізнаності чи інші супутні фактори, що спричиняють людські помилки, буде приводити ледь не до 70% від всіх інцидентів та кібератак на хмарну інфраструктуру. [12] Для прикладу, користувачі можуть використовувати невідомі чи сторонні незахищені інтерфейси прикладного програмування (API),

ненавмисно створюючи слабкі місця по периметру хмари, залишаючи конфіденційні ресурси повністю відкритими для кібератак.

5. Шкідливе програмне забезпечення

Доволі розповсюдженим міфом вважається повна захищеність від традиційних атак шкідливим програмним забезпеченням(ШПЗ) після міграції даних у хмару. Хоч і ціллю таких атак будуть ПХП, кінцеві користувачі все одно відчуватимуть наслідки. Прикладом такої атаки буде гіперджекінг [13], коли відбувається підміна гіпервізорів – одних з будівельних блоків хмарних технологій, - на їх пошкоджені версії. Внаслідок даних маніпуляцій, зловмисники можуть як і викрасти дані, скомпрометувати облікові записи користувачів для розповсюдження ШПЗ чи виконання фішингових атак.

6. Викрадення облікових записів

Як і у випадку з традиційною IT інфраструктурою, викрадення облікових записів здебільшого відбувається через слабкі парольні політики або недбале їх зберігання кінцевими користувачами, через що ми можемо вважати даний ризик одним з видів людських помилок. Якщо ж паролем діляться з іншими чи записують його в нотатках, то ймовірність отримати доступ до електронної пошти, а звідти - до хмарного аккаунту, зростає в експоненціальній швидкості. Але оскільки приблизно до третини всіх корпоративних даних у хмарному сховищі мають доступ всі користувачі, то облікові записи стають ще більш бажаною ціллю для зловмисників.

7. Інсайдерські атаки

Атаки зсередини інформаційних систем набули неабиякої актуальності як для традиційної, так і хмарної інфраструктур. Це можуть бути підкуплені працівники, необачні у своїх діях користувачі або ж суб’єкти загроз, які отримали довіру наївних працівників. За даними звіту 2022-го року Proofpoint кількість інсайдерських інцидентів зросла на 44% всього за два роки і очевидно, що вона лише збільшується. [14] Таке зростання здебільшого має зв’язок з популяризацією віддаленої роботи, або ж впровадженням політики використання власних пристроїв BYOD.

Існує, звісно, безліч інших ризиків, але всі вони ведуть, здебільшого, до витоку даних і як було наголошено в розділі 1, більше половини таких інцидентів виникли саме через людські помилки або інсайдерські атаки. Та й розслідування Verizon за 2023 рік стверджує даний факт, адже 74% витоків даних були пов’язані з людиною, а саме з крадіжкою облікових даних співробітників. [15]

Для прикладу, візьмемо звіт 2023 року команди дослідників Sysdig TRT, які проаналізували серію атак на хмарну інфраструктуру фінансових та телекомунікаційних організацій зловмисного угрупування TeamTNT. В якості отримання доступу до хмари, вони постійно шукали або місконфігурації чи вразливості у веб-додатках, або досліджували хмарні сховища за допомогою сканувань чи брутфорсу, як-от AWS S3 «бакети», в яких часто зберігаються різноманітні ключі та секрети. Отримавши певні облікові дані вже за лічені хвилини зловмисники отримали доступ до багатьох корпоративних ресурсів, видозмінили політики безпеки і ескалювались до ролі адміністратора.

Таким чином, можна було легітимно пересуватись по всій хмарній інфраструктурі, разом з тим, як і отримати доступ до наземних серверів, якщо такі існують і вони під’єднані до хмари. [16]

Найбільшою проблемою, з якою стикаються команди безпеки, є те, що більшість рішень з захисту хмарних технологій не завжди дають повну видимість не тільки місконфігурацій, але й прав та дозволів суб’єктів на об’єкти. Через це аналітикам потребується близько двох тижнів, щоб виявити скомпрометовані об’єкти в системі та відреагувати на певного характеру інцидент.

Відповідно для того, щоб зрозуміти, яким чином проактивно захищати хмарну інфраструктуру і постійно знищувати існуючі шляхи атак, набула неабиякої актуальності та поширення така політика безпеки Zero Trust.

1.2 Політика безпеки Zero Trust та її використання у хмарних середовищах

Контроль доступу у хмарній безпеці – це своєрідна система, яка дозволяє організаціям регулювати та контролювати дозволи й доступ до корпоративних даних, розробляючи різні політики, які підходять під індивідуальні потреби організацій. І для захисту даних вкрай необхідно правильно налаштовувати моделі керування доступу в хмарі, адже це дає компаніям можливість знизити ймовірність отримання певних прав несанкціонованим користувачам і, в той же час, надати достатній рівень привілеїв для безперебійного функціонування бізнес-процесів.

У зв’язку з цим була розроблена політика безпеки Zero Trust, яку можна описати коротким висловом «ніколи не довіряй і завжди перевіряй». Дану модель можна охарактеризувати як інструмент проактивного захисту хмарного середовища, адже для її досягнення необхідно дотримуватись трьох основних принципів:

1. Постійно й ретельно проводити автентифікацію та авторизацію

Аби уникнути компрометації облікових записів, необхідно надавати доступ з певними правами до об’єкти лише верифікованим користувачам. Для цього рекомендується виконувати авторизацію на основі всіх доступних атрибутів користувача, включаючи його ідентифікацію, місцезнаходження, стан пристрою, службу та ін.

2. Використовувати принцип найменших привілеїв

Обмежувати доступ користувачів за допомогою інструментів Just-in-Time, адаптивних політик доступу на основі ризиків та захисту даних. Це дає змогу співробітникам мати лише необхідний для них рівень прав та дозволів на певні хмарні ресурси, що відповідно знижує ймовірність інсайдерських атак та порушень конфіденційності чи цілісності корпоративних даних.

3. Знати й мінімізовувати поверхню атак

Для отримання повної картини безпеки хмарного середовища організації, варто проводити постійні сканування та оцінку власної поверхні атак на предмет вразливостей, а також обмежувати інтернет-доступ важливих для бізнесу активів. [17]

Організації неабияк підвищили свою експертизу у адмініструванні такої служби як Active Directory у традиційній IT інфраструктурі, що також слугує інструментом контролю доступу суб'єктів до об'єктів і надає можливість впроваджувати принципи найменших привілеїв. Проте практика використання даних у хмарі показала, що цього недостатньо для регулювання прав і дозволів користувачів для всіх об'єктів у хмарному середовищі на основі моделей RBAC чи ABAC.

Все тому, що здебільшого, адміністратори хмари нехтують налаштуваннями політик доступу, вважаючи, що ПХП все зробив замість них. Це, у свою чергу, породжує проблему виникнення великої кількості надлишкових прав для користувачів і суперечить головним принципам Zero Trust.

Для цього ПХП створили додаткові сервіси по моніторингу та аудиту всіх користувачів, ролей, груп безпеки і сервісних облікових записів та усіх прав та дозволів, що вони мають і в рамках мого дослідження були проаналізовані послуги від Amazon AWS.

1.3 Підтримка Zero Trust сервісами Amazon AWS

Отримати повну видимість активності користувачів у хмарі AWS та їх будь-які права доступу можна за допомогою таких чотирьох основних сервісів:

1. AWS IAM Access Analyzer

Даний сервіс допомагає ідентифікувати активи у організації AWS, що містять певний публічний доступ для користувачів ззовні. На основі постійного моніторингу політик безпеки надає звіти по надлишковим правах доступу на певних ресурсах, що зображено на рисунку 1.4. Проте за допомогою такого аналізатора досить складно отримати інформацію про стан доступів всередині організації. [18]

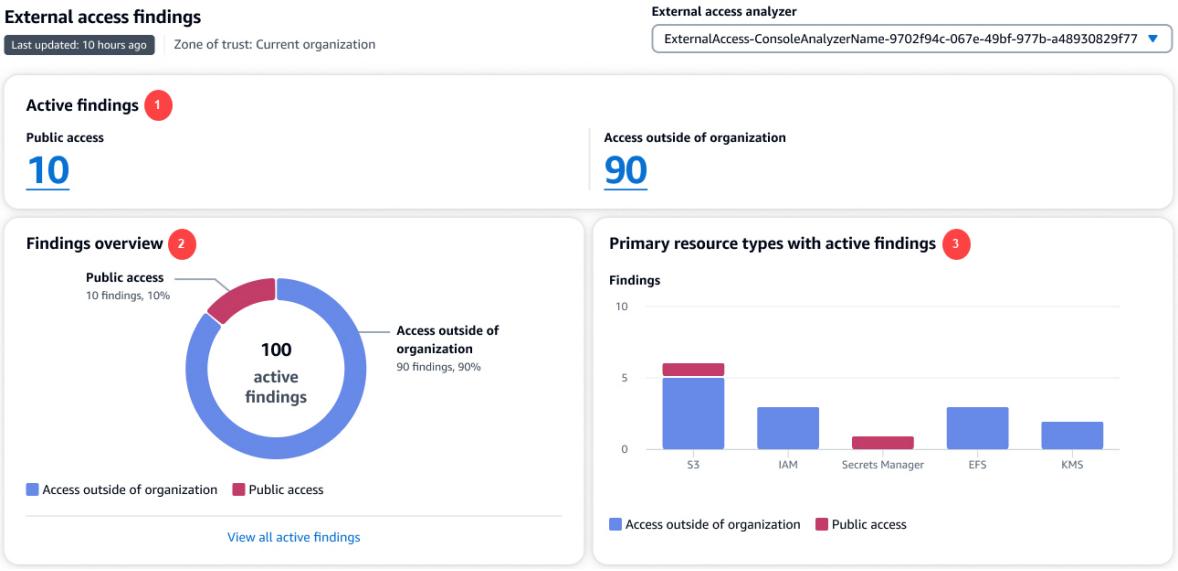

Рисунок 1.4 – Інформаційні панелі сервісу AWS IAM Access Analyzer

2. AWS IAM Policy Simulator

Даний інструмент допомагає адміністратору AWS організації тестувати нові чи існуючі політики доступу користувачів на ресурси. Проте для його стабільної роботи необхідно провести ряд налаштувань і врахувати обмеженість його функціоналу. Для прикладу, зміни політик, проведені під час симуляції, не будуть примінятись до існуючих, а також такого роду тестування вважається не дуже ефективним в рамках великих середовищ. На рисунку 1.5 зображено результат роботи симуляції для користувача. [19]

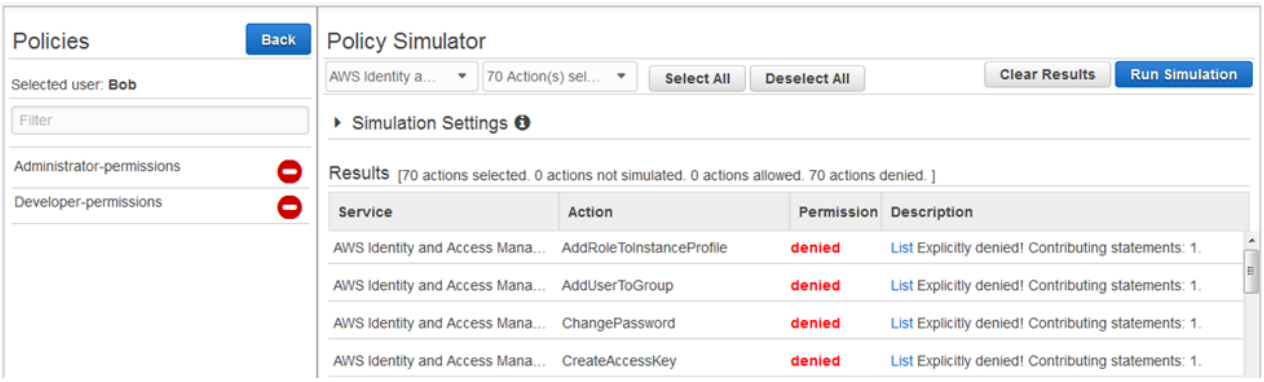

Рисунок 1.5 – Симуляція політики доступу на AWS IAM для користувача Bob

3. AWS CloudTrail

Даний сервіс є аналогом журналу подій, адже він також моніторить та логує всі дії користувачів у обліковому записі AWS. Його принцип роботи зображено на рисунку 1.6. На його основі можна відстежувати активність користувачів та виявляти аномальні поведінки. Проте зчитування логів не надає прямої інформації про надлишкові права й дозволи. А також адміністратору буде необхідно проводити аналіз великого обсягу подій, що є доволі неефективним процесом.

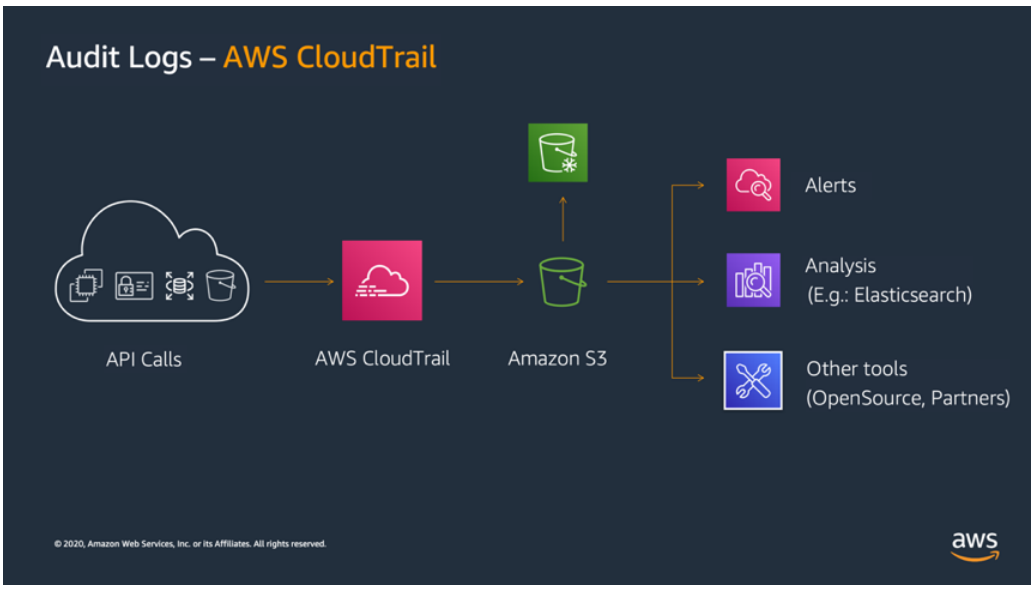

Рисунок 1.6 – Архітектура Cloud Trail [20]

4. AWS Config

За допомогою даного інструменту можливо відстежувати конфігурації доступу ресурсів у хмарі на відповідність політикам безпеки провайдера , а також

і політикам доступу IAM. Сервіс надасть можливість побачити надлишкові права доступу, але дуже обмежено та й, здебільшого, функціонал AWS Config зосереджений саме на виявленні проблем конфігурацій після проведення певних додаткових налаштувань, що зображено на рисунку 1.7.

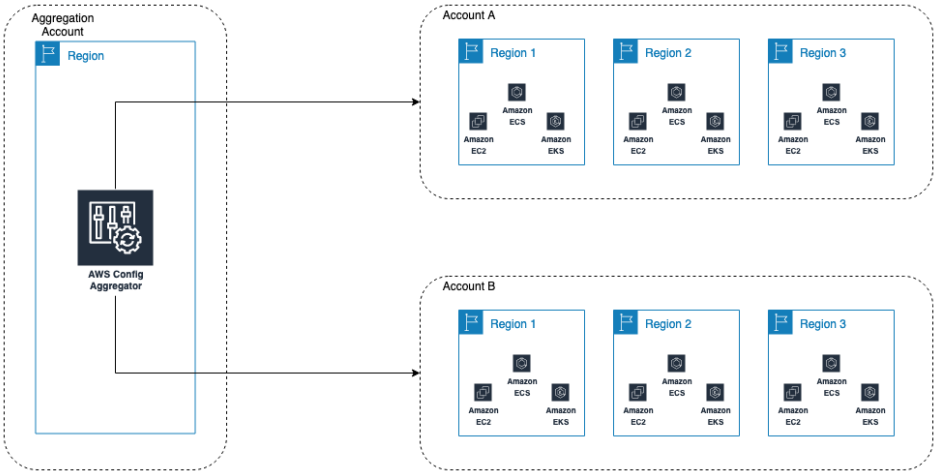

Рисунок 1.7 - Елементи, що перевіряє сервіс AWS Config [21]

Проаналізувавши дані нативні методи виявлення надлишкових прав, одразу можна виокремити проблеми, які будуть виникати у хмарних адміністраторів організацій. І це породило вимогу створити такий клас рішень з кібербезпеки хмарних середовищ, який буде аналізувати всю інформацію з облікових записів AWS та надавати кінцевому користувачеві детальний опис усіх ресурсів у хмарі.

Таким класом став CIEM, основна задача якого ідентифікувати надлишкові права й дозволи, надати рекомендації стосовно імплементації принципу найменших привілеїв та, за вимоги, власноруч генерувати такі політики доступу

Висновки до розділу 1

Хмарні технології сьогодні вважаються однією з найбільш домінуючих парадигм в сфері інформаційних технологій. Вона пропонує ряд нових, відносно

дешевих сервісів, такі як програмне забезпечення як послуга (SaaS), інфраструктура як послуга (IaaS) та платформа як послуга (PaaS) та інші, що значно спрощують організаціям управління наземними обчислювальними ресурсами. Проте, незважаючи на досить підвищену ефективність та гнучкість у користуванні, все ще виникають проблеми безпеки, що включають в собі захищеність конфіденційних даних, інсайдерські атаки, недбале використання хмарних сервісів та, звісно ж, кібератаки. І останні роки показали, що однією з фундаментальних вимог безпеки хмарних ресурсів є саме притримання принципів політики безпеки Zero Trust, які значно зменшують можливості несанкціонованого доступу до конфіденційних ресурсів компаній.

Під час переходу організацій до Zero Trust адміністратори хмари зіштовхуються з рядом проблем автоматизації, адже вручну проаналізувати всі наявні права та дозволи користувачів на ресурси практично неможливо в умовах стрімкого масштабування. Для цього хмарні провайдери надають свої певні сервіси, проте практично усі з них є фрагментарними й вимагають складних налаштувань. Через це виник новий клас рішень з хмарної безпеки CIEM, який агрегує та аналізує дані з усього хмарного середовища і надає чіткі рекомендації по усуненню вразливостей рівня Identity.

Хоч і основний функціонал CIEM-систем доволі широкий і значно переважає над використанням точкових сервісів ПХП, проте виникає питання у його ефективності для впровадження політики Zero Trust у хмарних середовищах організацій.

2 ОПИС ТЕХНОЛОГІЇ CIEM-СИСТЕМ. ФОРМУВАННЯ КРИТЕРІЇВ ТА ВИБІР МЕТОДУ ОЦІНКИ ЕФЕКТИВНОСТІ

2.1 Аналіз функціоналу рішення класу CIEM – Tenable Cloud Security

Так як основний функціонал CIEM-систем у будь-яких рішень однаковий, було прийнято рішення про проведення аналізу лише одного такого комерційного продукту - Tenable Cloud Security. Власне процес дослідження можливостей було поділено на декілька етапів:

1. Вивчення документації та початок роботи з рішенням
2. Аналіз виявленої та відображеної інформації у консолі управління
3. Ведення звітності

Задля підключення рішення до облікового запису організації, згідно документації, необхідно створити додаткову IAM роль з певними правами, що залежать від потреби власника облікового запису AWS. Рішення може виконувати різний функціонал опираючись на тип підключення, яких є основних 2 – read-only та read-write, що зображено на рисунку 2.1.

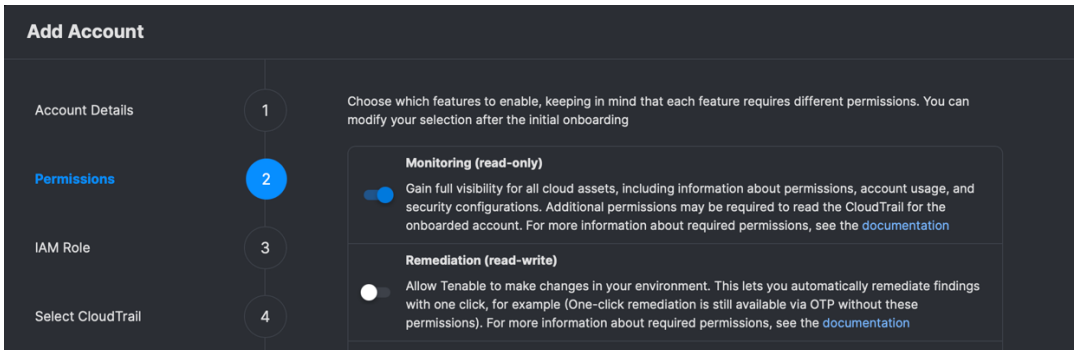

Рисунок 2.1 - Варіанти підключення AWS облікового запису до рішення

Надавши бажаний доступ до середовища AWS, рішення починає сканувати хмарну інфраструктуру за допомогою відправки API запитів, які є нативними для

AWS. На даному етапі було відзначено легкість імплементації та створення додаткового ризику для організації у випадку використання read-write підключення.

Так як одним з головних принципів політики Zero Trust є сканування поверхні атаки та проведення інвентаризації активів організації, наступним нашим кроком у аналізі рішення було саме відображення виявлених об’єктів.

На рисунку 2.2 зображено інвентаризацію об’єктів у тестовому обліковому записі AWS і варто зазначити, що ми одразу можемо бачити у табличному форматі коротку інформацію про той чи інший об’єкт/суб’єкт залежного від його типу та рівень виявлених у них вразливостей.

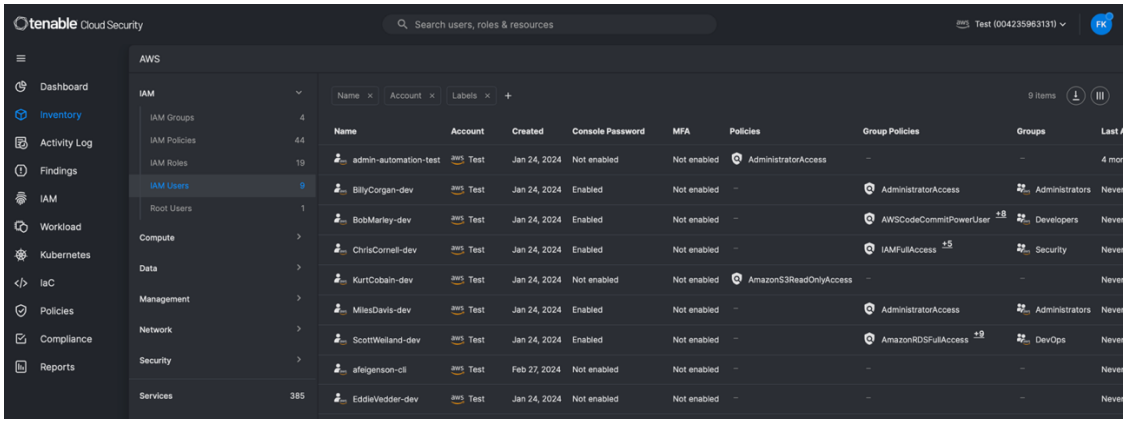

Рисунок 2.2 - Панель інвентаризації хмарних ресурсів

Так як нас в першу чергу цікавить виявлення надлишкових прав, то для їх відображення необхідно було зануритись у деталі кожного суб’єкту у хмарі, а саме: IAM ролі, користувачі, групи та політики. Дана інформація відображається у форматі графу для кожного суб’єкта окремо та приклад зображений на рисунку 2.3.

Якщо ж ми бачимо певні вразливості на тому чи іншому суб’єкті, що стосується надлишкових прав, то ми можемо побачити рекомендації по їх усуненню, а також і вивантажити виправлену політику доступу. Власне порівняти ці політики доступу можна прямо з консолі, що відображено на рисунку 2.4

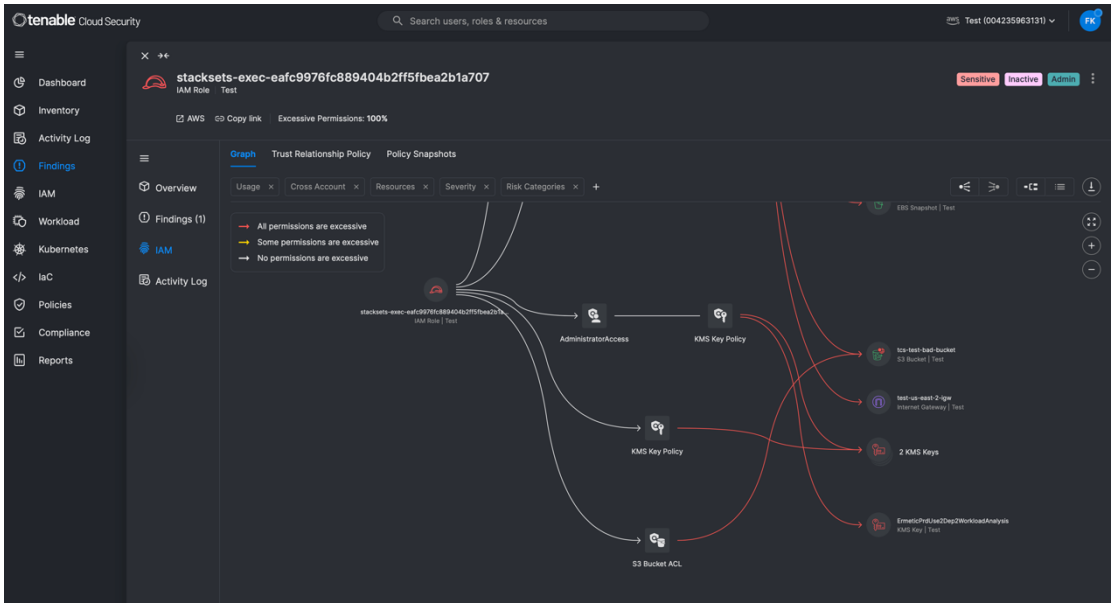

Рисунок 2.3 - Графічне зображення виявлених надлишкових прав

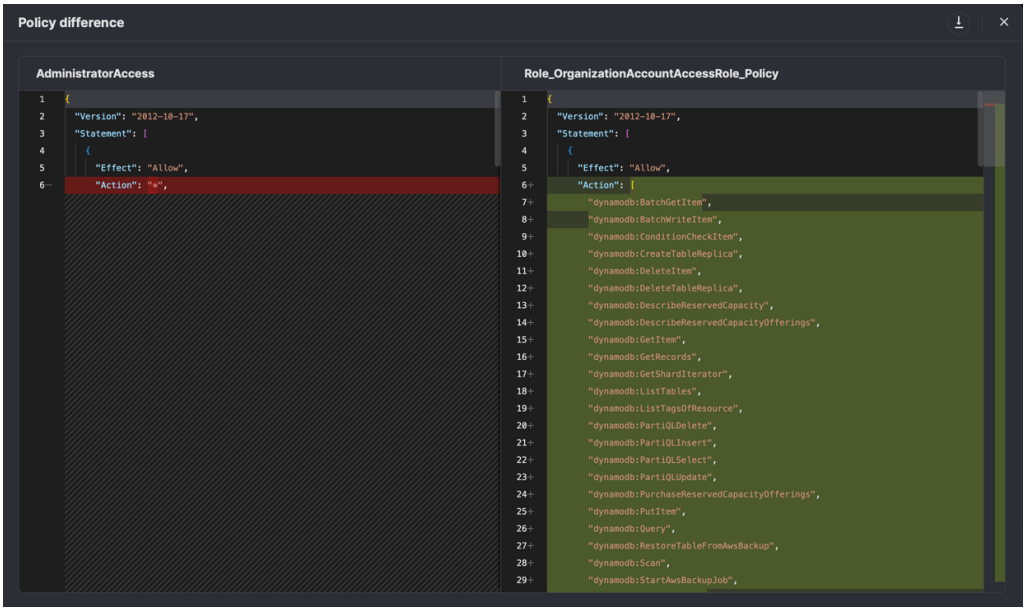

Рисунок 2.4 - Різниця між проблемною та виправленою політиками доступу

Також для зручності впровадження Zero Trust було виявлено можливість самостійної генерації політик доступу керуючись принципом найменших привілеїв, що можна побачити на рисунку 2.5. Дану політику згодом можна скопіювати та змінити існуючу безпосередньо в обліковому записі AWS.

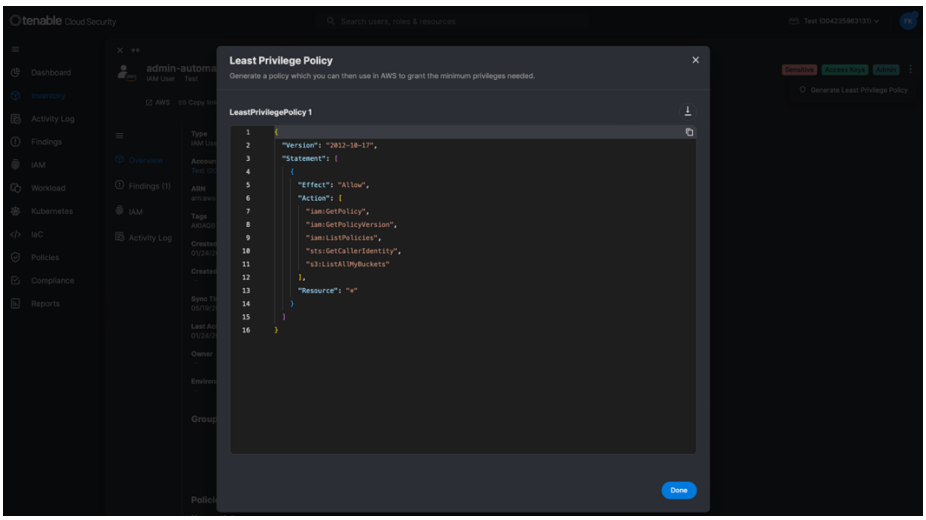

Рисунок 2.5 - Генерація політики доступу керуючись найменшими необхідними привілеями

Одним з головних вимог до CIEM-систем була глибина сканування облікового запису AWS і відображення політик безпеки для кожного хмарного ресурсу, їх взаємодію тощо. Тому у функціоналі рішення було знайдено пункт про версії політик безпеки, що зображено на рисунку 2.6. Так як Tenable Cloud Security сканує середовище кожну годину, то ми досить швидко змогли побачити і зміни у створених правах й дозволах користувачів.

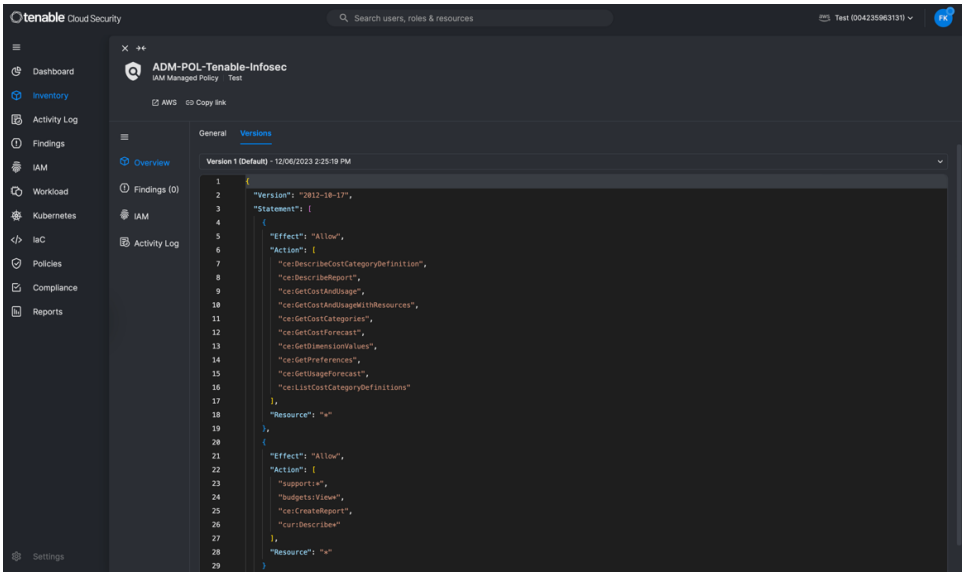

Рисунок 2.6 - Відображення політик доступу та їх версії з часом створення

Проте незважаючи на такий досить глибокий функціонал та аналітику, перебирати велику кількість хмарних ресурсів, хоч і в одній консолі, забирає досить багато часу. Тому ми вирішили проаналізувати звітність та саме відображення результатів сканувань у зібраному вигляді.

Для цього у рішенні існує окрема панель меню “IAM”, що відображена на рисунках 2.7 та 2.8, де ми можемо у табличному та візуалізованому форматі отримати критичну інформацію.

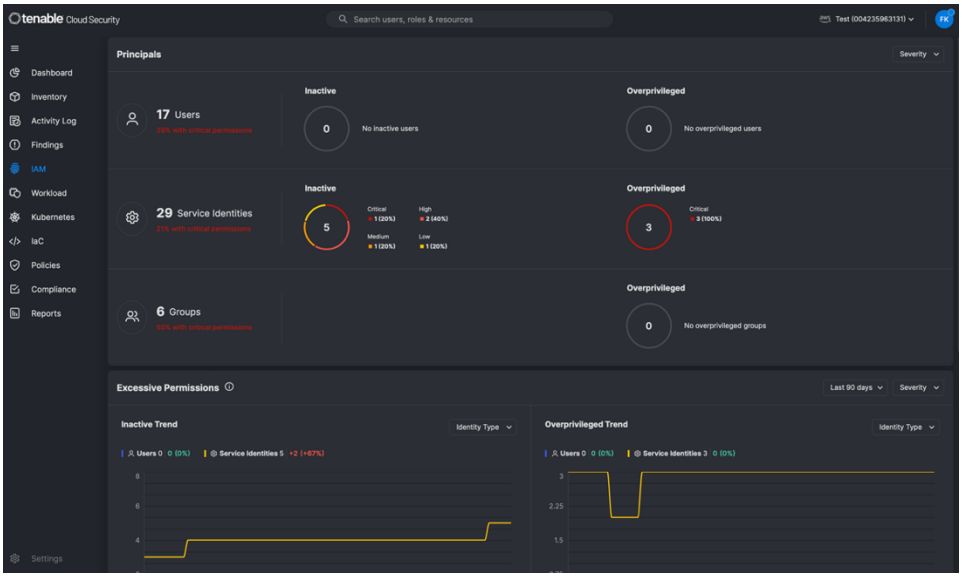

Рисунок 2.7 - Панель меню “IAM” з інформаційними панелями

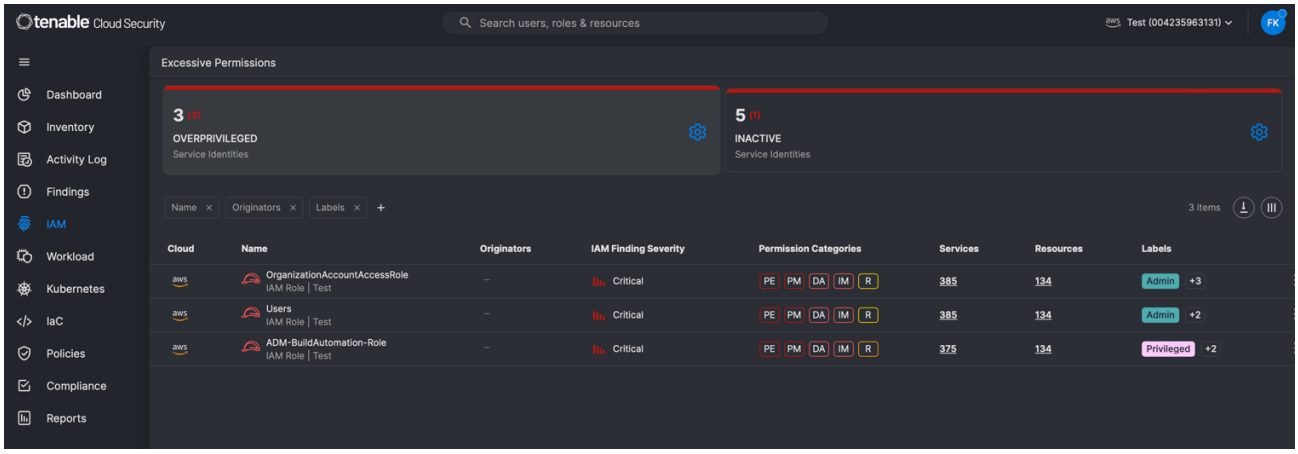

Рисунок 2.8 - Панель меню зі списком надлишкових прав та неактивних користувачів

Одним з пунктів аналізу була можливість надання тимчасових прав за допомогою інструментів JiT Access, де ми змогли дозволяти певні дії користувачам на конкретний об’єкт. Результат роботи даного інструменту відображений на рисунку 2.9.

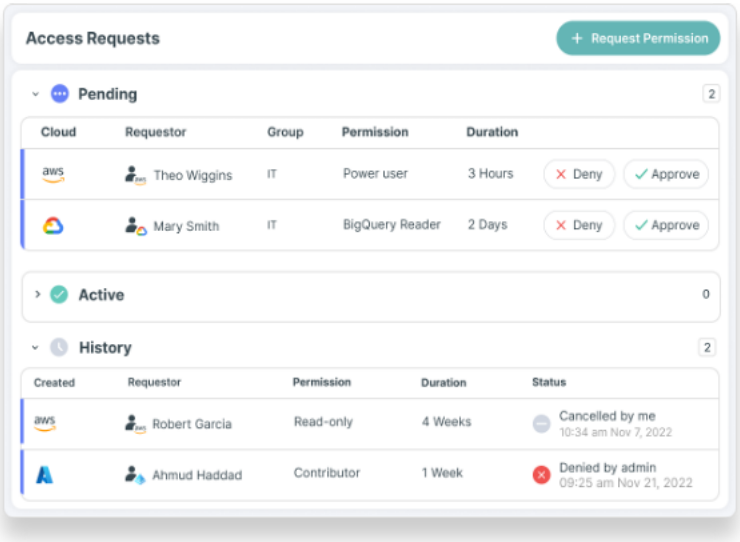

Рисунок 2.9 - Панель інструменту Just-in-Time Access

2.2 Визначення критеріїв для оцінки експертами ефективності роботи з даним рішенням в рамках впровадження політики Zero Trust

Враховуючи загальний функціонал CIEM рішень проаналізований на основі комерційного продукту Tenable Cloud Security були визначені певні критерії оцінювання ефективності роботи даного рішення в рамках імплементації політики Zero Trust у хмарні середовища AWS організацій:

1. Реалізація принципів найменших привілеїв;

Наскільки ефективно даний клас рішень допомагає у впровадженні принципів найменших привілеїв для прав і дозволів користувачів у хмарному середовищі.

2. Виникнення ризиків внаслідок інтеграції з даним рішенням;

Чи створюються нові вразливості на поверхні атаки організації внаслідок впровадження CIEM-систем у їх хмарну інфраструктуру.

3. Проведення інвентаризації інфраструктури;

Наскільки глибоким та повним можна назвати сканування хмари організації.

4. Відображення суб’єктів - користувачів, їх груп та ролей;

Наскільки зручним є відображення суб’єктів хмарного середовища у консолі управління та надання детальної інформації про кожен з цих суб’єктів.

5. Аналіз політик доступу кожного об’єкту в середовищі;

Чи відображаються версії політик у консолі управління та чи можна їх співставити водночас з суб’єктами, хто отримав певні дозволи на той чи інший об’єкт.

6. Ідентифікація надлишкових прав суб’єктів на об’єкти;

Наскільки тривалий процес вивчення поведінки суб’єктів задля виявлення надлишкових прав і з якою точністю вони визначаються.

7. Наявність покрокових рекомендацій по усуненню проблем у політиках керування доступом;

Можливість відображення проблем безпеки чи неправильних налаштувань у політиках доступу, а також генерації на певний час політик за принципом найменших привілеїв.

8. Підтримка надання тимчасових прав на певні ресурси.

Зручність використання інструментів JiT Access задля надання суб’єкту, що запросив доступ, необхідних йому прав та дозволів на короткий термін часу.

Дані критерії , виходячи з їх опису, мають певний зв’язок між собою, який зображено на рисунку 2.10.

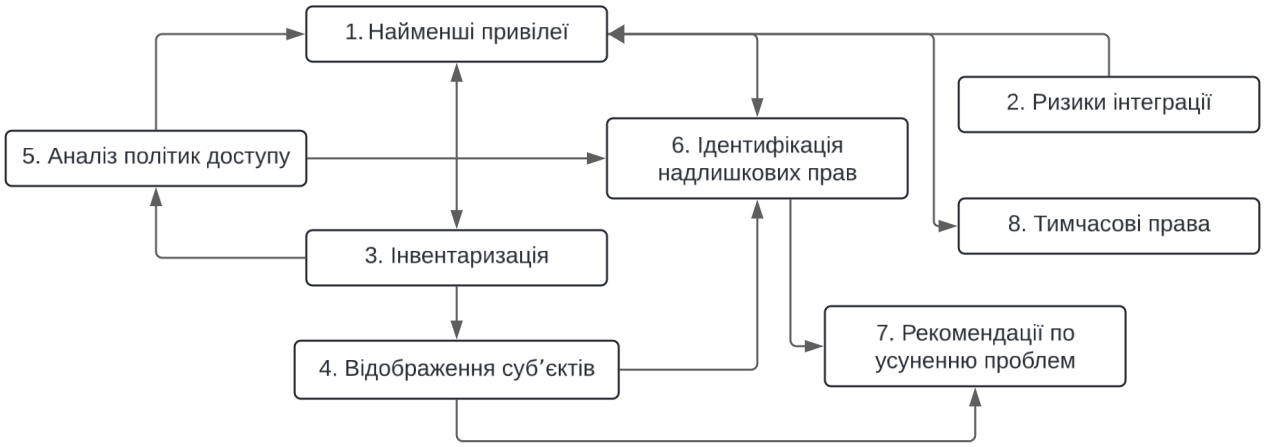

Рисунок 2.10 – Діаграма взаємозв'язків критеріїв оцінювання

Розглянемо детальніше ці зв'язки:

1. Реалізація принципів найменших привілеїв

На даний критерій впливає ряд інших під номерами 2, 5, а також існує і взаємозв'язок з критеріями 6, 3 та 8, проте основна суть зв'язків полягає у наданні CIEM-системами можливостей виявлення надлишкових прав та дозволів, налаштування видачі тимчасових прав, перевірки політик доступу хмарних ресурсів та мінімізації ризиків внаслідок інтеграції з хмарним середовищем користувача. І все це так чи інакше впливає на реалізацію принципів найменших привілеїв, роблячи її тривалішою, дещо складнішою чи навпаки.

2. Аналіз політик доступу має зв'язок з ідентифікацією надлишкових прав та дозволів, адже залежно від того, наскільки глибоко проводиться аналіз активності користувачів та їх використання певних привілеїв згідно з призначеними їм політиками, будуть виявлятись проблеми доступу.

3. Інвентаризація впливає на аналіз політик доступу та відображення суб'єктів у хмарі внаслідок проведення постійного сканування та моніторингу середовища і відображення будь-яких змін у консолі управління.

4. Відображення усіх суб'єктів та максимально повної інформації про них має прямий зв'язок з ідентифікацією надлишкових прав та наданні рекомендацій по усуненню такого роду проблем безпеки.

5. Ідентифікація надлишкових прав впливає на рекомендації по усуненню проблем, адже вони повинні повністю інтегруватись в хмарне середовище користувачів і не бути абстрактними. А це, у свою чергу, залежить і від правильного виявлення проблем безпеки та надання деталізованого контексту про них.

Задля ефективного проведення оцінювання CIEM-систем згідно заданих критеріїв необхідно звернутись до методів багатокритеріального аналізу, аби підібрати найбільш вдалий для нашого випадку.

2.3 Методи багатокритеріального аналізу

Багатокритеріальний аналіз прийняття рішень (MCDA) — це аналітичний метод, що застосовується для прийняття рішень у ситуаціях, де потрібно враховувати декілька різних критеріїв чи судження багатьох експертів. Даний метод забезпечує гнучкість у прийнятті рішень завдяки охопленню широкого спектру методів, які дозволяють всіляко оцінювати і порівнювати альтернативи, враховуючи раніше визначені критерії чи вимоги, що висуваються до них. MCDA зазвичай поєднує в собі якісні та кількісні елементи:

1. **Якісний елемент** має на увазі взаємодію з експертами, тобто їх оцінка своїх знань, досвіду та суб'єктивного сприйняття, і яка може бути виражена через шкали (наприклад, високий, середній, низький) або інші форми якісної інформації;
2. Коли як **кількісний елемент** включає в собі власне критерії оцінки виражені у числовому форматі. [22]

   Основні етапи багатокритеріального аналізу зображені на рисунку 2.11.

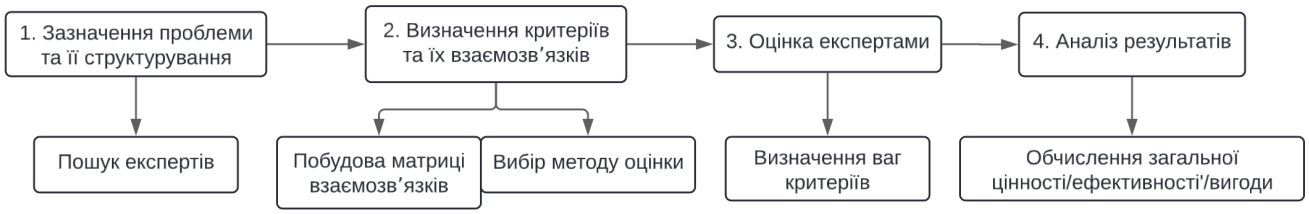

Рисунок 2.11 – Діаграма етапів багатокритеріального аналізу

Розглянемо кожен з цих етапів детальніше:

1. Зазначення проблеми та її структурування

Даний етап передбачає постановку проблеми, ідентифікацію її ключових елементів, специфіку та відповідний пошук експертів у потрібній галузі проведення оцінки та фінального прийняття рішення.

2. Визначення критеріїв та їх взаємозв'язків

На даному етапі формуються критерії оцінювання, визначаються певні взаємозв'язки між ними, та залежно від даних параметрів визначатиметься метод проведення оцінювання експертами.

3. Оцінка експертами

Проводиться оцінювання експертами критеріїв відповідно до поставленої проблематики. Після збору даних визначаються ваги критеріїв для визначення їх важливості, а також до результатів застосовується обраний на попередньому етапі метод оцінювання.

4. Аналіз результатів

Даний завершальний етап включає в собі узагальнення оцінки ефективності/вигоди/цінності у розрізі проблематики та відповідне прийняття рішення.

Даний процес MCDA може бути доволі варіативним, зокрема при виборі методу оцінювання. Наразі методів існує безліч, проте найвідомішими з них є AHP, TOPSIS, ELECTRE, PROMETHEE, ANP та інші. Розглянемо детальніше три з них:

2.3.1. AHP

Метод аналізу ієрархій (MAI) - це теорія, розроблена Томасом Сааті для вимірювання критеріїв шляхом попарного порівняння з використанням суджень за шкалою від 1 до 9 і результуючого визначення пріоритетності(ваг) цих ж критеріїв.

Метод можна застосовувати як до матеріальних, так і до нематеріальних критеріїв і найкраще він себе проявляє, коли необхідно прийняти рішення опираючись саме на важливість критеріїв. Саме ж прийняття рішення відбувається шляхом побудови ієрархічної моделі, яка включає мету, критерії та альтернативи, після чого формуються попарні порівняння суджень щодо переваги певного елементу над іншим.

Якщо розглянути принцип роботи з даним методом, то після побудови ієрархічної моделі нам необхідно створити попарні матриці порівняння критеріїв $К_1$, $К_2$, …, $К_n$ за шкалою від 1 до 9, де 1 означає однакову важливість, а 9 – абсолютну перевагу. Сама матриця порівнянь $A = [a_{ij}]$, де a_{ij} – перевага критерію $К_i$ над $К_j$, виглядатиме, як зображено на таблиці 2.1:

Таблиця 2.1 – Матриця попарних порівнянь

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \cdots & 1 \end{bmatrix}$$

Наступним кроком необхідно провести нормалізацію матриці, тобто кожен елемент матриці А необхідно поділити на суму елементів у стовпці, до якого він належить. І останнім етапом необхідно знайти середнє арифметичне елементів кожного рядка, що буде слугувати результуючими вагами пріоритетності критерію або ж його власним значенням. [23]

2.3.2 TOPSIS

TOPSIS - це метод багатокритеріального аналізу, розроблений у 1981 році Чінг-Лай Хвангом та Юн Кунгом. Він базується на принципі вибору альтернативи, яка має найменшу евклідову відстань до ідеального рішення та найбільшу до негативного ідеалу.

Цей метод є досить корисним у випадках, коли необхідно прийняти рішення про найкращу альтернативу, опираючись на певні критерії та їх важливість, як приклад можна вважати прийняття рішення про купівлю авто чи вибір стратегії розвитку підприємства.

Для того, аби скористатись даним методом, необхідно спершу скласти матрицю порівняння альтернатив та їх критеріїв, що зображена у таблиці 2.2, а також визначити вектор ваг (власний вектор) для критеріїв W = (w_1, w_1, …, w_n), де w_j означає важливість критерію K_j.

Таблиця 2.2 – Матриця порівнянь альтернатив та їх критеріїв

$$\begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} K_1 & K_2 & \dots & K_n \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \end{array},$$

де $K_1, K_2, \dots, K_n$ – критерії порівняння;

$A_1, A_2, \dots, A_m$ – альтернативи;

a_{ij} – характеристика альтернативи A_i за критерієм K_j.

Потім з отриманими вхідними даними варто пронормувати матрицю за наступною формулою:

$$r_{ij} = \frac{a_{ij}}{\sqrt{\sum_{k=1}^{m} a_{kj}^2}} \qquad (2.1)$$

де $\sum_{k=1}^{m} a_{kj}^2$ – арифметична сума елементів стовпця.

А також помножити кожен елемент нормованої матриці на відповідні критерію ваги.

Наступним етапом буде визначення позитивних та негативних ідеальних рішень. Для цього варто обрати критерії, що позитивно впливають на прийняття рішення - множина J і навпаки – множина J′, та об’єднати найсприятливіші значення для нас у вектори ідеальних рішень I^+ та I^-. Такий розподіл відбувається за наступною формулою:

$$I^+ = \{v_1^*, \dots, v_n^*\} \qquad (2.2)$$

де $v_j^* = \{Max_i(v_{ij}) \text{ if } j \in J; Min_i(v_{ij}) \text{ if } j \in J'\}$.

Аналогічно і для множини I^-, тільки $v_j^{'} = \{Min_i(v_{ij}) \text{ if } j \in J; Max_i(v_{ij}) \text{ if } j \in J'\}$.

Отримавши дані вектори розраховується евклідова відстань альтернатив до ідеальних рішень та відносна відстань за формулою 2.3

$$C_i^* = \frac{S_i^-}{S_i^- + S_i^+}; \quad 0 < C_i^* < 1 \qquad (2.3)$$

де S_i^- та S_i^+ - евклідові відстані альтернатив A_i до негативного та позитивного ідеальних рішень відповідно.

Результативна відносна відстань, яка має значення, найближче до 1, і є нашою найкращою альтернативою. [24]

2.3.3 ANP

ANP вважається певним розширенням методу AHP, розроблене Томасом Сааті задля врахування складних взаємозв'язків між елементами ієрархії. Дане вдосконалення дозволяє враховувати як зворотні, так і прямі залежності критеріїв.

Власне знайома ієрархічна структура методу AHP дещо змінює свою форму і набуває мережевої структури. Тобто все елементи в рамках цієї мережі

взаємодіють один з одним, а відображається даний зв’язок у вигляді кластерів та вузлів.

Сам принцип роботи з даним методом полягає у наступних кроках:

1. Визначення мети, критеріїв та альтернатив;

2. Побудова мережевої структури критеріїв, визначення їх взаємозв’язків, розбиття на кластери;

3. Побудова матриць порівнянь елементів для кожного кластеру та між кластерами у мережі, що мають ідентичний вигляд матриць зображених у таблиці 2.1 Порівняння відбувається за шкалою від 1 до 9, що аналогічне аналізу у методі AHP;

4. Визначення у матрицях векторів ваг та формування на їх основі суперматриці елементів, що має вигляд як у таблиці 2.3;

Таблиця 2.3 – Суперматриця взаємозв’язків елементів у мережі

$$W = \begin{array}{c} \\ C_1 \\ C_2 \\ \vdots \\ C_n \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nn} \end{bmatrix} \end{array}$$

Де C_i – кластер мережі, що складається з елементів (критеріїв)

5. Нормалізація суперматриці та її узагальнення граничних пріоритетів для отримання обмеженої суперматриці. Як правило, для узагальнення використовується наступна формула 2.4:

$$\lim_{k\to\infty} W^k \qquad (2.4)$$

6. Фінальна нормалізація обмеженої суперматриці та отримання глобальних ваг елементів мережі. [25]

Висновки до розділу 2

CIEM-системи наразі не є широковживаним рішенням безпеки хмарної інфраструктури, через що власне й виникає необхідність у дослідженні їх можливостей. Як приклад такої системи був проаналізований комерційний продукт Tenable Cloud Security.

Функціонал такого рішення надає широку аналітику стосовно існуючих хмарних ресурсів. Адміністратор може не перемикатись між купою сервісів AWS, а лише в одній панелі побачити детальну інформацію про власні хмарні ресурси, та й скористатись можливостями автоматизації, що в купі додають неабиякої зручності та легкості під час впровадження Zero Trust в моделі керування доступом організації.

Як результат аналізу функціоналу CIEM-систем були визначені 8 критеріїв, що є взаємопов’язаними і для їх ефективного оцінювання було необхідно звернутись до методів багатокритеріального аналізу.

У висновку, метод аналізу мереж (ANP) є найбільш вигідним для задач, де існують складні взаємозв'язки між критеріями, що особливо важливо у контексті нашого дослідження. Тому його було обрано для подальшої оцінки ефективності CIEM-систем як інструменту виявлення надлишкових прав та дозволів у хмарних середовищах організацій.

3 ЗАСТОСУВАННЯ РОЗРОБЛЕНОЇ МЕТОДИКИ ДЛЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ CIEM-СИСТЕМ В ХОДІ ІМПЛЕМЕНТАЦІЇ ZERO TRUST

3.1 Підготовка вхідних даних та аналіз критеріїв для методу аналітичних мереж

Для початку роботи з методом ANP необхідно провести аналіз мережевої структури та розібратись з метою, критеріями та альтернативами. Критерії були визначені у 2-му розділі, то ж перейдемо до формування мети та альтернатив:

Мета полягає в оцінці ефективності CIEM рішень для впровадження організаціями політики Zero Trust у їх хмарну інфраструктуру.

Альтернатива у нашому випадку лише одна, а саме CIEM рішення, доцільність і ефективність використання яких підпадає оцінюванню.

Для побудови мережі необхідно згрупувати критерії з їх взаємозв’язками у *кластери*. Це нам дасть можливість формувати матриці попарних порівнянь критеріїв всередині кластеру та самих кластерів у мережі. З рисунку 2.10 можна сформувати мережу зв’язків критеріїв, яка зображена на рисунку 3.1.

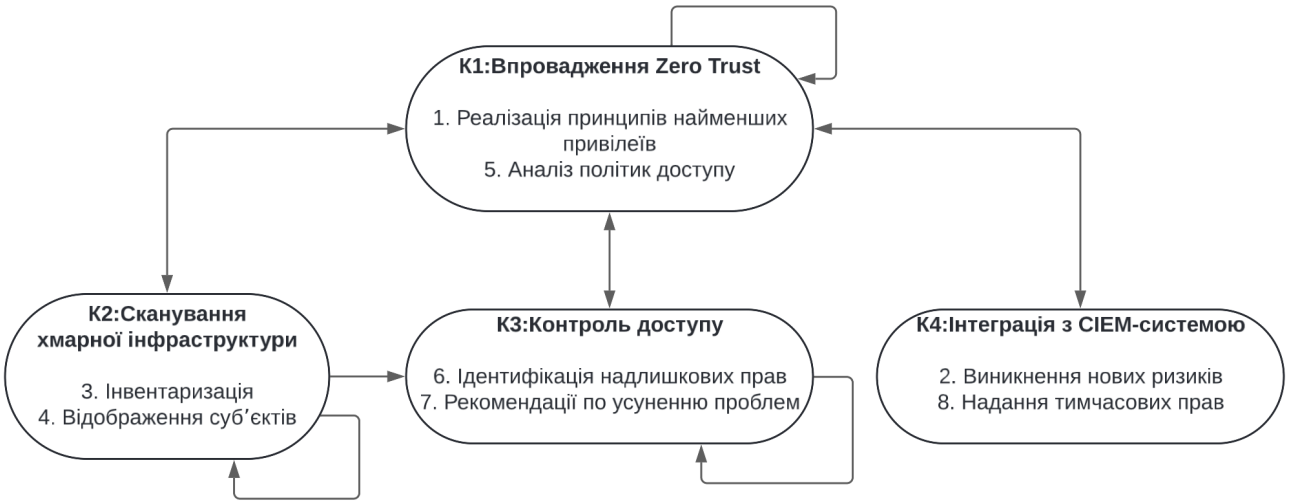

Рисунок 3.1 – Діаграма взаємозв’язків кластерів елементів мережевої структури

З рисунку видно, що кластери, в які ми згрупували критерії, взаємодіють між собою, а саме:

Елементи кластеру 1 мають як прямий так і зворотній зв’язки з елементами кластерів 2,3 та 4, а також елементи впливають на одне одного всередині кластеру. Елементи К2 мають прямий зв’язок з елементами К3, а також зворотній з К2, що означає вплив елементів одне на одного всередині кластеру. Елементи К3 також впливають одне на одного в межах кластеру.

Суперматриця для даної мережі виглядатиме наступним чином, як на таблиці 3.1:

	Кластер	**К1**		**К2**		**К3**		**К4**	
Кластер	Критерій	1	5	3	4	6	7	2	8
К1	1	W11		W12		W13		W14	
	5								
К2	3	W21		W22		W23		W24	
	4								
К3	6	W31		W32		W33		W34	
	7								
К4	2	W41		W42		W43		W44	
	8								

Суперматриця складається з ряду менших матриць w_{ij}, $i,j=\overline{1,4}$, які формуються шляхом попарних порівнянь елементів кластерів і розрахунку їх ваг. Попарні порівняння елементів у мережі відбуваються за принципом оцінювання важливості одного елементу над іншим за шкалою від 1 до 9, де 1 означає однакову важливість, а 9 – абсолютну перевагу. Згодом цю матрицю необхідно нормалізувати і обчислити їх ваги. На таблиці 3.2 зображено матриці порівнянь для знаходження w11, w12, w13, w14.

Таблиця 3.2 – Результати розрахунків матриць попарних порівнянь для w11,w12,w13,w14 по критеріях

№1	**1**	**5**	**Ваги**
1	1	1/2	0.333
5	2	1	0.667
№5	**1**	**5**	**Ваги**
1	1	3	0.75
5	1/3	1	0.25
№3	**1**	**5**	**Ваги**
1	1	1/5	0.166
5	5	1	0.834
№4	**1**	**5**	**Ваги**
1	1	1	0.5
5	1	1	0.5
№6	**1**	**5**	**Ваги**
1	1	1	0.5
5	1	1	0.5
№7	**1**	**5**	**Ваги**
1	1	1/4	0.2
5	4	1	0.8
№2	**1**	**5**	**Ваги**
1	1	4	0.8
5	1/4	1	0.2

Продовження таблиці 3.2

№8	**1**	**5**	**Ваги**
1	1	6	0.857
5	1/6	1	0.143

Розрахунки для матриць w21,w22,w23,w24 представлені у таблиці 3.3
Таблиця 3.3 – Матриці попарних порівнянь для w21,w22,w23,w24

№1	**3**	**4**	**Ваги**
3	1	5	0.834
4	1/5	1	0.166
№5	**3**	**4**	**Ваги**
3	1	1/3	0.25
4	3	1	0.75
№3	**3**	**4**	**Ваги**
3	1	2	0.667
4	1/2	1	0.333
№4	**3**	**4**	**Ваги**
3	1	1/4	0.2
4	4	1	0.8
№6	**3**	**4**	**Ваги**
3	1	3	0.75
4	1/3	1	0.25
№7	**3**	**4**	**Ваги**
3	1	1	0.5
4	1	1	0.5

Продовження таблиці 3.3

№2	**3**	**4**	**Ваги**
3	1	1	0.5
4	1	1	0.5
№8	**3**	**4**	**Ваги**
3	1	1	0.5
4	1	1	0.5

Розрахунок матриць попарних порівнянь для w31,w32,w33,w34 наведено у таблиці 3.4

Таблиця 3.4 – Матриця попарних порівнянь для w31,w32,w33,w34

№1	**6**	**7**	**Ваги**
6	1	6	0.857
7	1/5	1	0.143
№5	**6**	**7**	**Ваги**
6	1	3	0.75
7	1/3	1	0.25
№3	**6**	**7**	**Ваги**
6	1	2	0.667
7	1/2	1	0.333
№4	**6**	**7**	**Ваги**
6	1	2	0.667
7	1/2	1	0.333
№6	**6**	**7**	**Ваги**
6	1	4	0.8
7	1/4	1	0.2

Продовження таблиці 3.4

№7	**6**	**7**	**Ваги**
6	1	1/3	0.25
7	3	1	0.75
№2	**6**	**7**	**Ваги**
6	1	1	0.5
7	1	1	0.5
№8	**6**	**7**	**Ваги**
6	1	1	0.5
7	1	1	0.5

У таблиці 3.5 зображено останні розрахунки матриць попарних порівнянь для знаходження w41,w42,w43.

Таблиця 3.5 – Матриця попарних порівнянь для w41,w42,w43

№1	**2**	**8**	**Ваги**
2	1	6	0.857
8	1/6	1	0.143
№5	**2**	**8**	**Ваги**
2	1	1	0.5
8	11	1	0.5
№3	**2**	**8**	**Ваги**
2	1	1	0.5
8	1	1	0.5
№4	**2**	**8**	**Ваги**
2	1	1	0.5
8	1	1	0.5

Продовження таблиці 3.5

№6	**2**	**8**	**Ваги**
2	1	2	0.667
8	1/2	1	0.333
№7	**2**	**8**	**Ваги**
2	1	4	0.8
8	1/4	1	0.2

Сформована суперматриця за результатами розрахунків матриць попарних порівнянь зображена у таблиці 3.6

Таблиця 3.6 – Суперматриця елементів мережі

	Кластер	**К1**		**К2**		**К3**		**К4**	
Кластер	**Критерій**	**1**	**5**	**3**	**4**	**6**	**7**	**2**	**8**
К1	**1**	0.333	0.75	0.166	0.5	0.5	0.2	0.8	0.857
	5	0.667	0.25	0.834	0.5	0.5	0.8	0.2	0.143
К2	**3**	0.834	0.25	0.667	0.2	0.75	0.5	0.5	0.5
	4	0.166	0.75	0.133	0.8	0.25	0.5	0.5	0.5
К3	**6**	0.857	0.75	0.667	0.667	0.8	0.75	0.5	0.5
	7	0.143	0.25	0.333	0.333	0.2	0.25	0.5	0.5
К4	**2**	0.857	0.5	0.5	0.5	0.667	0.8	0	0
	8	0.143	0.5	0.5	0.5	0.333	0.2	0	0

Наступні кроки передбачають проведення обрахунків з даною суперматрицею, а саме її нормалізацію та узагальнення границь її значень.

3.2 Програмна реалізація використання методу аналітичних мереж за допомогою Python

Так як дана матриця є достатньо великою і вести математичні обрахунки вручну займає тривалий період часу, було прийнято рішення автоматизувати їх шляхом програмної реалізації.

Задля цього ми скористались мовою програмування Python, а саме її бібліотеками pyanp та numpy. Бібліотека pyanp була створена для спрощення проведення процесу прийняття рішень з використанням методів AHP та ANP. За допомогою неї ми можемо обчислити глобальні ваги критеріїв через певні маніпуляції з суперматрицею.

Для цього нам необхідно нормалізувати суперматрицю так, щоб сума кожного стовпця була рівна 1 та піднести її до стаціонарного вигляду. Тому скористаємось модулем бібліотеки pyanp – limitmatrix. Даний модуль дозволяє в рамках однієї функції піднести матрицю до максимально можливого степеню, коли зміни значень між ітераціями практично не будуть змінюватись, а також і пронормувати її. Задля цього нам необхідно було викликати функцію *pyanp.limitmatrix.calculus(<назва матриці>)*

Результат нормування та підведення матриці до стаціонарного вигляду зображений у таблиці 3.7

Таблиця 3.7 – Нормалізована та обмежена суперматриця

№ критерію	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0,083	0,188	0,044	0,125	0,125	0,05	0,267	0,286
2	0,167	0,062	0,22	0,125	0,125	0,2	0,067	0,048
3	0,208	0,062	0,176	0,05	0,188	0,125	0,167	0,167
4	0,042	0,188	0,035	0,2	0,062	0,125	0,167	0,167
5	0,214	0,188	0,176	0,167	0,2	0,188	0,167	0,167

Продовження таблиці 3.7

6	0,036	0,062	0,088	0,083	0,05	0,062	0,167	0,167
7	0,214	0,125	0,132	0,125	0,167	0,2	0	0
8	0,036	0,125	0,132	0,125	0,083	0,05	0	0

Обчислимо глобальні ваги критеріїв за допомогою використання модулю бібліотеки pyanp – priority, а саме функції *pyanp.priority.pri_eigen(<назва матриці>).* Дана функція виконує автоматизований пошук власних векторів або ж вагів у матриці шляхом певних обчислень, як у методі AHP. Визначений власний вектор критеріїв з нормалізованої суперматриці зображений у таблиці 3.8:

Таблиця 3.8 – Глобальні ваги критеріїв

№ критерію	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Ваги	0,146	0,127	0,143	0,123	0,183	0,089	0,12	0,069

Отримані ваги означають завершення аналізу методом аналітичних мереж, тому з даним результатом можна переходити до обчислення загальної оцінки ефективності впровадження CIEM-систем організаціями в ході імплементації політики Zero Trust у їх хмарну інфраструктуру. Також лістинг програмного коду, задіяного під час дослідження методом аналітичних мереж, наведено у додатку А.

3.3 Оцінка ефективності рішень контролю керування доступом експертами

Задля проведення оцінки згідно вказаних у розділі 2 критеріїв було залучено 15 експертів, які протягом місяця часу тестували CIEM рішення від різних розробників. Оцінка позначалась цілим числом від 1 до 5, де:

1. – повністю незадоволений/функціонал відсутній;
2. – частково незадоволений;

3. – невизначено;

4. – частково задоволений;

5. – повністю задоволений;

У ході опитування отримали результати, що вказані у таблиці 3.9:

Таблиця 3.9 – Оцінки експертів згідно критеріїв

№ експерту \ № критерію	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	3	4	5	3	4	2	3	1
2	5	1	4	4	1	2	5	2
3	5	3	4	3	2	1	4	2
4	3	3	3	5	4	3	4	1
5	5	4	4	2	2	4	5	1
6	4	4	3	2	3	5	3	4
7	3	5	5	3	5	5	4	1
8	3	3	5	3	5	2	5	1
9	4	3	4	3	5	4	4	5
10	2	1	5	4	2	3	4	3
11	3	1	5	4	3	2	4	2
13	5	5	2	3	4	2	4	1
14	4	4	4	3	4	4	2	2
15	5	4	5	5	4	1	4	4

Для отримання загальної оцінки ефективності, нам необхідно провести певні проміжні обрахунки, що зображені у таблиці 3.10:

1. Обчислити середні значення даних оцінок по критеріях;

2. Помножити їх на ваги критеріїв, отриманих у підрозділі 3.2;

3. Просумувати отримані числа для отримання загальної оцінки

Таблиця 3.10 – Проміжні обрахунки для отримання загальної оцінки ефективності

№ критерію	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Середня оцінка по критерію	4	3,5	4	3	4	2,5	4	2
Зважена оцінка	0,584	0,4445	0,572	0,369	0,732	0,2225	0,48	0,138
Сума зважених оцінок	3,542							

Нормалізуємо дану суму зважених оцінок, використавши формулу 3.1:

$$\frac{3{,}542}{5} * 100\% = 71\ \% \qquad (3.1)$$

Отримане значення у відсотках і є нашою загальною оцінкою ефективності використання CIEM-систем організаціями для імплементації політики Zero Trust у їх хмарні середовища.

3.4 Розробка методичних рекомендацій по використанню CIEM для впровадження організаціями політики Zero Trust у хмарі AWS

Після аналізу отриманої оцінки ефективності та визначення рівня задоволеності експертами було розпочато роботу над методичними рекомендаціями по використанню такого класу рішень у хмарних середовищах організації. Наразі список рекомендацій налічує близько 7 пунктів:

1. Додавати можливості автоматизації для рішення, аби усувати надлишкові права безпосередньо з консолі управління;
2. Проводити комплексну оцінку ризиків поверхні атаки перед впровадженням CIEM;
3. Регулярно формувати звіти по інвентаризації хмарної інфраструктури, щоб відслідковувати зміни;
4. Підвищувати експертизу у адмініструванні Amazon AWS, щоб отримувати ще більше розуміння атрибутів об’єктів у консолі CIEM-системи;
5. Проводити аналіз усіх проблем безпеки та пріоритизувати їх;
6. Використовувати CIEM-системи у комплексі з іншими рішеннями безпеки хмарної інфраструктури;
7. Заздалегідь обирати бажані облікові записи організації для моніторингу і розробити матрицю ролей з правами доступу для користувачів консолі CIEM.

Висновки до розділу 3

У даному розділі дипломної роботи було проведено практичне дослідження ефективності впровадження систем керування доступом (CIEM) організаціями у ході імплементації політики Zero Trust у їх хмарні інфраструктури. Отримання загальної оцінки було проведено у декілька етапів, а саме визначення глобальних ваг критеріїв, оцінювання експертами та обробка результатів.

Задля виконання першого етапу було використано метод аналітичних мереж, який передбачав створення мережевої моделі критеріїв та їх взаємозв'язків, формування матриць попарних порівнянь та інші кроки, що є специфічними для даного методу. У результаті було сформовано суперматрицю, що враховувала взаємодію критеріїв у мережевій моделі, і на її основі обраховано глобальні ваги.

Зокрема, операції з суперматрицею проводились з використанням бібліотеки pyanp мови програмування Python, що неабияк спростила процес аналізу.

Як результат аналізу методом ANP були отримані глобальні ваги, які ми використали для обчислення загальної оцінки ефективності. Для отримання більш об'єктивної оцінки було проведено також опитування 15 експертів, які мали змогу протестувати CIEM-системи у власних хмарних інфраструктурах.

На основі отриманих результатів було встановлено, що ефективність досягла 71%. Задля покращення ефективності і поширення CIEM-систем серед організацій були розроблені рекомендації по безпеці користування даним класом рішень в ході впровадження політики Zero Trust.

ВИСНОВКИ

Використання рішень із захисту хмарної інфраструктури на рівні прав та дозволів ще не є доволі розповсюдженою практикою в Україні, проте ефективність її використання була неодноразово доведена під час тестувань комерційних продуктів, як-от Tenable Cloud Security, організаціями.

Сам процес оцінки ефективності класу рішень CIEM є доволі довготривалим, адже він потребує глибокого аналізу потреб на ринку, бажаного функціоналу та залучення достатньої вибірки експертів. Власне такою потребою була розглянута імплементація політики Zero Trust у хмарні середовища, адже більшість організацій зіштовхуються з проблемами безпеки пов’язаних саме з занадто привілейованими користувачами чи надмірною кількістю непотрібних прав та дозволів.

Дані ризики можливо мінімізувати за допомогою вбудованих сервісів хмарного провайдеру Amazon AWS, проте всі вони є дуже фрагментарними та не надають повної картини безпеки у хмарній інфраструктурі шляхом синхронізаціїї одне з одним.

Розглянувши можливості CIEM-систем у розрізі підготовки до впровадження Zero Trust було визначено 8 критеріїв оцінювання ефективності, однак, враховуючи їх взаємозв’язки, постає проблема формалізації багатокритеріального вибору. Для її вирішення у ході дослідження було залучено метод аналітичних мереж та його часткову програмну реалізацію з використанням бібліотеки pyanp мови python. Поєднавши результати аналізу даним методом і експертне оцінювання, було встановлено загальну оцінку ефективності впровадження CIEM-систем у хмарні середовища організацій, яка становить 71%.

Загалом, CIEM-системи досить сильно спрощують роботу адміністраторів та команд безпеки з аналізу поверхні атак хмарної інфраструктури, проводити її моніторинг та вчасно реагувати на загрози чи інциденти, пов’язані з Identity частиною хмари. Також суттєво покращується і проактивний підхід до управління

вразливостями, тому розроблені рекомендації лише спростять адміністрування рішень класу CIEM і дозволять отримати всебічне розуміння власної інфраструктури, яка постійно масштабується.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) The Relationship Between IoT and Cloud Computing [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.cloudpanel.io/blog/iot-and-cloud-computing/#the-relationship-between-iot-and-cloud-computing
2) Cloud Computing in 2024: Unveiling Transformations and Opportunities [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://www.forbes.com/sites/emilsayegh/2024/01/02/cloud-computing-in-2024-unveiling-transformations-and-opportunities/?sh=a07f1908e773
3) Private Access to AWS-hosted SaaS applications [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/use-case-examples.html
4) Worldwide Public Cloud End-User Spending Forecast [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240
5) The Rise of Cloud Computing and Its Impact on IT Infrastructure [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://medium.com/@parker123/the-rise-of-cloud-computing-and-its-impact-on-it-infrastructure-d3f76daa43c3
6) Cloud Migration Strategies [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/cloud/what-is-a-cloud-migration-strategy.html#~strategies
7) Cloud Security Report ISC2 [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.isc2.org/-/media/Project/ISC2/Main/Media/Marketing-Assets/CCSP/2023-Cloud-Security-Report-ISC2_final.pdf
8) Cloud Computing Statistics [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.cloudwards.net/cloud-computing-statistics/

9) Cloud Security Research [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://cpl.thalesgroup.com/cloud-security-research#download-popup

10) Cloud Computing Security Risks and Security Measures [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://online.york.ac.uk/cloud-computing-security-risks-and-security-measures/

11) Risks of Cloud Computing [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://builtin.com/articles/risks-of-cloud-computing

12) Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025 [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025

13) Virtual Machine Attacks and Cyber Resiliency [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.mitre.org/sites/default/files/publications/pr-16-3043-virtual-machine-attacks-and-cyber-resiliency.pdf

14) Cost of Insider Threats [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

15) 2023 Data Breach Investigations Report [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.verizon.com/business/resources/T4e/reports/2023-data-breach-investigations-report-dbir.pdf

16) 2023 Global Cloud Threat Report [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://sysdig.com/content/c/pf-2023-global-cloud-threat-report?x=u_WFRi

17) Zero Trust Model [Електронний ресурс]. – Режим доступу до ресурсу: https://www.microsoft.com/en-us/security/business/zero-trust

18) Identifying Unused Access [Електронний ресурс]. – 2024. – Режим доступу до ресурсу:https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html#what-is-access-analyzer-unused-access-analysis

19) Using IAM Policy Simulator [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html#policies_policy-simulator-how-it-works

20) Secure CloudTrail logs [Електронний ресурс]. – Режим доступу до ресурсу: https://maturitymodel.security.aws.dev/en/1.-quickwins/cloudtrail/

21) Vulnerability Assesment with AWS Config [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://aws.amazon.com/blogs/architecture/find-public-ips-of-resources-use-aws-config-for-vulnerability-assessment/

22) An Introductory Guide to MCDA [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://analysisfunction.civilservice.gov.uk/policy-store/an-introductory-guide-to-mcda/#section-1

23) Saaty, T.L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. – McGraw-Hill, 1980. – С. 19-55.

24) Hwang, C.L., Yoon, K. Multiple Attribute Decision Making: Methods and Applications. – Springer-Verlag, 1981. – С. 58-82.

25) Saaty, T.L. Decision Making with Dependence and Feedback: The Analytic Network Process. – RWS Publications, 1996. – С. 37-60.

ДОДАТОК А

ЛІСТИНГ ПРОГРАМИ

Лістинг програмного коду, розробленого для дослідження методом аналітичних мереж:

```
import numpy as np
from pyanp import priority
import pyanp.limitmatrix as lm


# суперматриця
supermatrix = np.array([
    [0.333, 0.75, 0.166, 0.5, 0.5, 0.2, 0.8, 0.857],
    [0.667, 0.25, 0.834, 0.5, 0.5, 0.8, 0.2, 0.143],
    [0.834, 0.25, 0.667, 0.2, 0.75, 0.5, 0.5, 0.5],
    [0.166, 0.75, 0.133, 0.8, 0.25, 0.5, 0.5, 0.5],
    [0.857, 0.75, 0.667, 0.667, 0.8, 0.75, 0.5, 0.5],
    [0.143, 0.25, 0.333, 0.333, 0.2, 0.25, 0.5, 0.5],
    [0.857, 0.5, 0.5, 0.5, 0.667, 0.8, 0, 0],
    [0.143, 0.5, 0.5, 0.5, 0.333, 0.2, 0, 0]
])
# Нормалізація
column_sums = supermatrix.sum(axis=0)
normalized_matrix = supermatrix / column_sums[np.newaxis, :]
normalized_matrix = np.round(normalized_matrix, decimals=4)


limited_supermatrix = lm.calculus(normalized_matrix)
print("Limited:\n", limited_supermatrix)
global_weights = priority.pri_eigen(l_matrix)
print("Global weights:", global_weights)
```