Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Моделювання безпечної архітектури хмарних сховищ»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Глазкова Олена Андріївна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Фесенко А.О.	

Нормоконтроль	Зюбіна Р. В.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** (група) **Глазковій Олені Андріївні** (прізвище ім'я по-батькові)

Тема дипломної роботи «Моделювання безпечної архітектури хмарних сховищ»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Статистичні данні про типи загроз хмарних сховищ, моделі хмарних сховищ, нормативно правова база, стандарти з хмарної безпеки

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Дослідити існуючі вразливості хмарних провайдерів сформувати вимоги відносно характеристик для роботи з хмарними сховищами, проаналізувати методи захисту, запропонувати технологічне рішення.

3

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Описане технологічне рішення готове до застосування для малого та середнього бізнесу при переході до хмарної інфраструктури.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 12 жовтня 2020 року.

Завдання видала	_____ (підпис)	А. О. Фесенко (ініціали, прізвище)
Завдання прийняв до виконання	_____ (підпис)	О.А. Глазкова (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1.	Аналіз літературних джерел	25.01.2021 - 20.02.2021	*виконано*
2.	Аналіз та опис проблематики	01.03.2021 - 20.03.2021	*виконано*
3.	Дослідження методів захисту хмарних сховищ	25.03.2021 - 01.04.2021	*виконано*
4.	Опис технологічного рішення	01.04.2021 - 05.04.2021	*виконано*
5.	Вироблення рекомендацій щодо використання засобу захисту	15.04.2021 - 02.05.2021	*виконано*
6.	Розробка архітектури та інтеграція рішень для побудови безпечного хмарного сховища	03.05.2021 - 10.05.2021	*виконано*
7.	Оформлення графічних матеріалів	11.05.2021 - 13.05.2021	*виконано*
8.	Оформлення презентації	15.05.2021 - 20.05.2021	*виконано*
9	Оформлення пояснювальної записки	01.06.2021 - 08.06.2021	*виконано*
10.	Підготовка до захисту	09.06.2021 - 21.06.2021	*виконано*

Завдання видав	_____ (підпис)	А.О. Фесенко (ініціали, прізвище)
Завдання прийняла до виконання	_____ (підпис)	О.А. Глазкова (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Моделювання безпечної архітектури хмарних сховищ» складається зі вступу, основної частини, що складається з трьох розділів, загальних висновків і списку використаних джерел. Загальний обсяг роботи складається з 79 сторінок. Робота містить 25 рисунків. Список використаних джерел включає 33 джерела.

Практичне значення роботи полягає в моделюванні комплексного рішення, яке може використовуватись суб'єктами при переході від фізичної інфраструктури до хмарного середовища з огляду на велику кількість умов, що повинні виконуватись для такого переходу. Архітектура хмарного сховища передбачає масштабування та використання структурами в рамках відповідності міжнародним нормативним документам з інформаційної безпеки.

Результати здійснених досліджень можуть бути використані для малого та середнього бізнесу, включаючи банки та фінансові організації.

Напрямки подальших досліджень можуть включати доопрацювання архітектури хмарних сховищ та впровадження додаткових алгоритмів захисту та нових механізмів моніторингу для фіксування інцидентів інформаційної безпеки.

Ключові слова: хмарні сховища, конфіденційна інформація, атаки, зберігання даних, безпека даних в хмарі, передача даних.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

SaaS	–	Software as a service
IaaS	–	Infrastructure as a service
PaaS	–	Platform-as-a-service
VPC	–	Virtual Private Cloud
NAT	-	Network address translation
DNS	–	Domain Name System
DLP	–	Data loss prevention
SDN	–	Software Defined Network
SIEM	–	Security Information and Event Management
SSO	–	Single Sign On
MFA	-	Multi-factor authentication
IAM	–	Identity and Access Management
API	–	Application Programming Interface
CSP	–	Content Security Policy
AI	–	Artifical Intelligence
PKI	–	Public Key Infrastructure
OCCI	–	Open Cloud Computing Interface
CIMI	–	Cloud Infrastructure Management Interface
SDG	–	Software-Defined Gateways
CASB	–	Cloud Access Security Brokers
WAF	–	Web Application Firewall
DDoS	–	Denial-of-Service
SSL	–	Secure Sockets Layer
ПЗ	–	Програмне Забезпечення

ЗМІСТ

ВСТУП

Актуальність полягає в тому, що інформаційна безпека піддається великим змінам в останні роки, особливо під натиском 21 століття та пандемії, оскільки все більше компаній переходять від фізичної інфраструктури до хмарної. У 90-х роках ділові та особисті дані жили на місцях - і безпека також була місцевою. Дані розміщуватимуться на внутрішньому сховищі ПК вдома та на корпоративних серверах, якщо ви працюєте в компанії.

Впровадження хмарних технологій змусило всіх переоцінити кібербезпеку. Ваші дані та програми можуть рухатися між локальною та віддаленою системами - і завжди доступні для Інтернету. Якщо ви отримуєте доступ до Документів Google на своєму смартфоні або використовуєте програмне забезпечення Salesforce для догляду за своїми клієнтами, ці дані можна зберігати де завгодно. Тому захистити його стає складніше, ніж тоді, коли мова йшла лише про те, щоб зупинити небажаних користувачів у доступі до вашої мережі. Хмарні обчислення існують приблизно два десятиліття, і, незважаючи на дані, що вказують на ефективність бізнесу, економічні вигоди та конкурентні переваги, значна частина бізнес-спільноти продовжує працювати без них. Згідно з дослідженням, проведеним Міжнародною групою даних, 69% підприємств уже використовують хмарні технології в тій чи іншій якості, а 18% заявляють, що в якийсь момент планують впровадити хмарні обчислювальні рішення. У той же час Dell повідомляє, що компанії, які інвестують у великі дані, хмари, мобільність та безпеку, отримують на 53% швидший ріст доходу, ніж їх конкуренти. Як показують ці дані, все більша кількість технічно підкованих підприємств та лідерів галузі усвідомлює безліч переваг хмарних обчислень. Але більше того, вони використовують цю технологію для більш ефективного управління своїми організаціями, кращого обслуговування своїх клієнтів та різкого збільшення загальної норми прибутку.

Проте, це не означає, що хакери та злочинці не адаптувалися до даного переходу, вони продовжують порушувати закон та діяти неправомірним чином, що ставить під загрозу всю інфраструктуру. Зазвичай компанії схильні недооцінювати

інформаційну безпеку, доки не стане надто пізно та вони не понесуть шалених збитків, які у більшості випадків є фатальними. Зараз говоримо не лише про фінансові витрати, але й про довіру користувачів, яка насправді є найбільш цінною. Оскільки, коли клієнт приходить до бізнесу, він віддає йому свою конфіденційну інформацію, та сподівається, що вона буде в повній безпеці, що на підприємстві працюють відповідальні та технічно-підковані спеціалісти та що вони потурбувалися, щоб вся їхня база даних клієнтів залишалася захищеною. Проте, якщо витік даних все-таки трапиться, довіра клієнтів буде втрачена назавжди, а це означає ніякого більше ніякого доходу.

Саме тому так важливо спеціалістам із кібербезпеки постійно йти в ногу з часом та підлаштовуватися під умови сучасності, що у наших реаліях означає інтегрувати засоби та заходи безпеки до хмарного середовища, щоб обумовити безпечну роботу та передачу даних в хмарі, при цьому не сповільнюючи, а навпаки підвищуючи ефективність вже робочої інфраструктури. Хмарна безпека - це дисципліна кібербезпеки, присвячена захисту хмарних обчислювальних систем. Сюди входить збереження конфіденційності та безпеки даних в Інтернет-інфраструктурі, програмах та платформах. Захист цих систем передбачає зусилля хмарних провайдерів та клієнтів, які їх використовують, незалежно від того, використовує це фізична особа, малий чи середній бізнес або підприємство.

Хмарні провайдери розміщують послуги на своїх серверах через постійне Інтернет-з’єднання. Оскільки їхній бізнес покладається на довіру споживачів, хмарні методи безпеки використовуються для забезпечення конфіденційності та безпечного зберігання даних клієнта. Однак безпека хмар також частково лежить і в руках клієнта. Розуміння обох аспектів є ключовим для здорового рішення хмарної безпеки. Хмарна безпека включає в себе цілий набір технологій, протоколів та найкращих практик, що захищають середовища хмарних обчислень, програми, що працюють у хмарі, та дані, що зберігаються в хмарі. Захист хмарних служб починається з розуміння того, що саме забезпечується, а також системних аспектів, якими потрібно керувати.

Як огляд, розробка серверних систем проти вразливих місць безпеки значною мірою знаходиться в руках постачальників хмарних послуг. Окрім вибору постачальника послуг, що забезпечують безпеку, клієнти повинні зосередитись переважно на правильній конфігурації послуг та звичках безпечного використання. Крім того, клієнти повинні бути впевнені, що обладнання та мережі кінцевого користувача належним чином захищені.

Отже, підходячи до висновку, підприємства визнають переваги хмарних обчислень і бачать, як вони впливають на їх виробництво, співпрацю, безпеку та дохід. Використовуючи хмарне рішення, підприємство може запобігти багатьом проблемам, які страждають від організацій, які покладаються на локальну інфраструктуру.

Об'єкт дослідження – процес безпечної передачі даних у хмарі.

Мета роботи – змоделювати комплексне рішення для мінімізації ризиків, пов'язаних із використанням хмарних сховищ.

Предмет дослідження – технологія керування даними у хмарних сховищах.

Методи дослідження – комплексний аналіз, структурний аналіз, порівняння, системний підхід, моделювання архітектури хмари.

РОЗДІЛ 1
АНАЛІЗ ТИПІВ АТАК НА ХМАРНІ СХОВИЩА ТА ОСНОВНІ МЕТОДИ ЇХ ПРОТИДІЇ ТА УСУНЕННЯ

1.1. Огляд сучасної позиції хмарних платформ

Під час пандемії багато спеціалістів зазначили розвиток хмарних сховищ. Пандемія змусила підприємства по всьому світу швидко переконфігурувати свою діяльність, щоб дати можливість своїм працівникам працювати віддалено, що полегшується завдяки застосуванню хмарних систем, отже криза COVID-19 зумовила та пришвидшила хмарний перехід: витрати на хмару зросли на 37% до 29 млрд. доларів протягом першого кварталу 2020 р. Ця тенденція, ймовірно, збережеться, оскільки вихід до віртуальної роботи підкреслює актуальність для легко масштабованих, безпечних, надійних, економічно вигідних послуг, що не потребують власних приміщень. Насправді, незважаючи на неминучий економічний спад внаслідок пандемії, хмарні витрати, за оцінками, зростуть на 19% за весь рік, навіть незважаючи на те, що, як прогнозує галузевий аналітик Gartner, витрати на IT в цілому скоротяться на 8%.

За даними 451 Research одна з найбільш затребуваних експертиз, але в той же час одна з найнедооціненіших являється експертиза в області хмарних платформ, як це показано на рисунку 1.1.

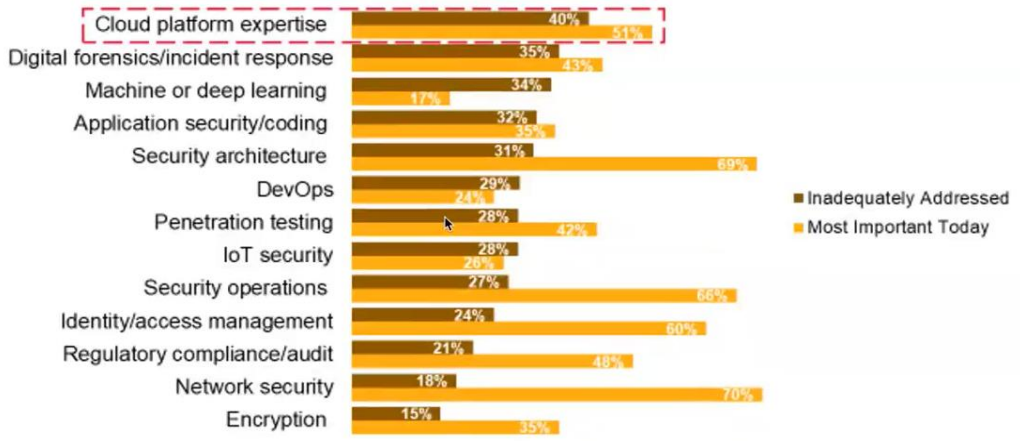

Рис.1.1 – Дослідження 451 Research з найбільш затребуваних експертиз

Також чому варто звернути увагу на хмарні сховища це те, що згідно з дослідженням, до кінця 2022 року половина всіх обчислень перейде в хмару. Звісно залишиться наземна інфраструктура, проте все більше процесів буде реалізована та автоматизована саме в хмарі. І хмарна безпека одна з основних трендів найближчих років, як це показано на рисунку 1.2.

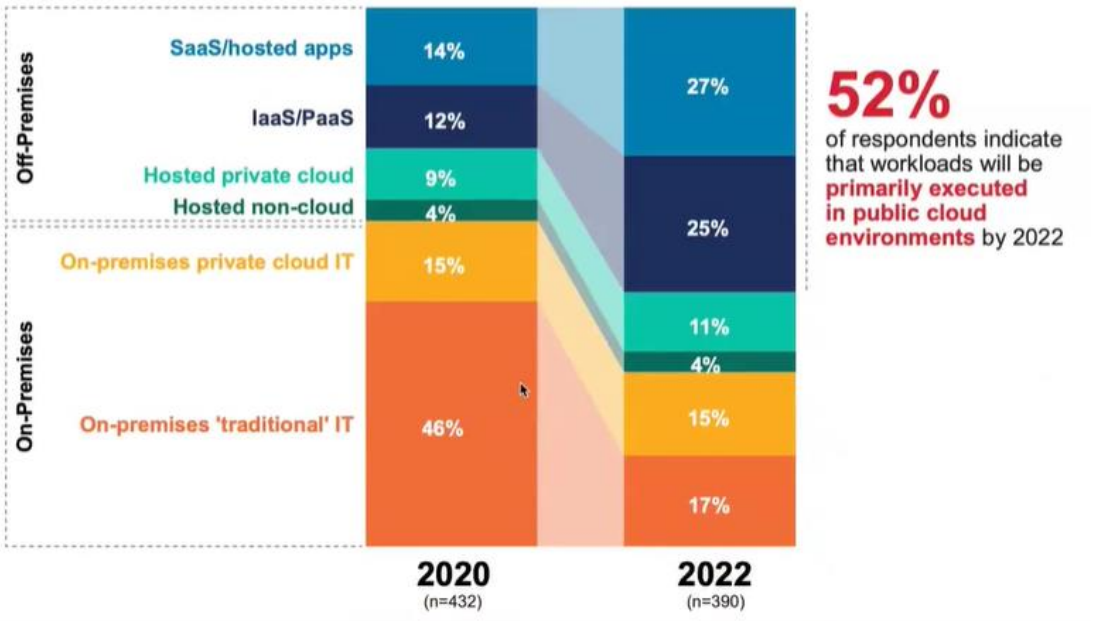

Рис.1.2 – Місце первинного робочого навантаження 2020-2022 (сукупний)

Як доказ, з точки зору куди підуть партнери та клієнти, та в що вони будуть інвестувати, на рисунку представлені дані, що найбільше інвестицій припадає саме на пошук нових співробітників, навчання та безпеку. Все більше буде інвестицій в сторону Managed Security Services, тобто в третю сторону яка забезпечуватиме безпеку та в SaaS security products. Окремо варто зазначити, що все менше компаній будуть витрачати гроші на програмно-апаратні комплекси, як це показано на рисунку 1.3.

Переходячи в хмару не потрібно забувати про проблеми та небезпеки, навіть, якщо хмара забезпечує багатьма інструментами в сфері безпеки, то все одно це не вирішить всі проблеми.

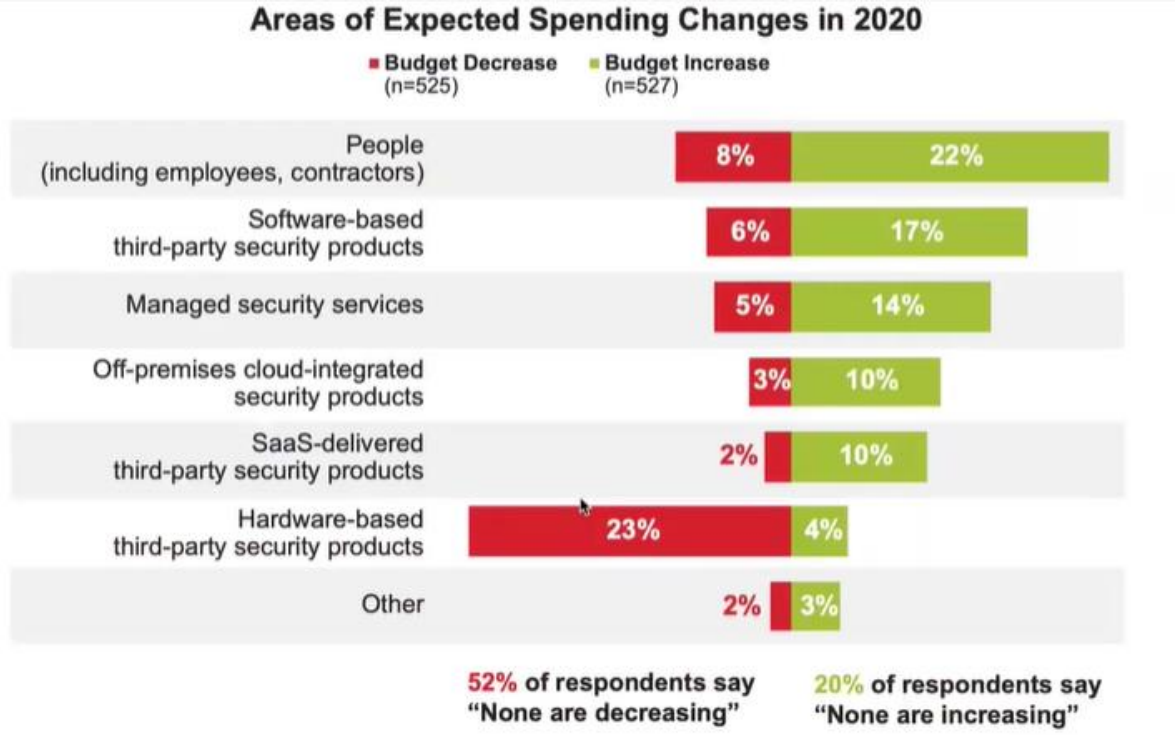

Рис.1.3 – Сфери змін витрат в 2020році

1.2. Найпоширеніші проблеми з точки зору безпеки

Хмарні обчислення представляють безліч унікальних проблем безпеки. У хмарі дані зберігаються у стороннього постачальника та доступ до них здійснюється через Інтернет. Це означає, що видимість та контроль над цими даними обмежені. Це також піднімає питання про те, як його можна правильно закріпити. Вкрай важливо, щоб кожен розумів свою роль і проблеми безпеки, властиві хмарним обчисленням. «Оцінка ризиків безпеки хмарних обчислень».

Гартнер зазначає у червневому звіті під назвою "Оцінка ризиків безпеки хмарних обчислень", що хмарні обчислення мають "унікальні атрибути, які вимагають оцінки ризику в таких сферах, як цілісність даних, відновлення та конфіденційність, а також оцінка юридичних питань у таких сферах, як електронне відкриття, відповідність нормативним актам та аудит", - говорить Гартнер.

1.3. Розподіл атак хмарних платформ за сервісами

Національний інститут стандартів і технологій (NIST) надає визначення хмарних обчислень та способи їх використання та розгортання.

NIST визначає такі характеристики та моделі для хмарних обчислень:

Основні характеристики: самообслуговування на вимогу, широкий доступ до мережі, об'єднання ресурсів, швидка еластичність та виміряне обслуговування

Сервісні моделі: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS)

Моделі розгортання: приватна хмара, публічна хмара та гібридна хмара.

В свою чергу, публічні хмарні сервіси розміщується сторонніми постачальниками хмарних послуг (наприклад, Amazon Web Services (AWS), Microsoft Azure, Google Cloud) і, як правило, доступні через веб-браузери, тому управління ідентифікацією, автентифікація та контроль доступу є важливими.

Наступна ланка - приватні хмари. Вони зазвичай цілеспрямовані і доступні лише для однієї організації. Однак вони все ще вразливі до порушень доступу, соціальної інженерії та інших вразливостей.

І на останок - гібридні хмари. Вони поєднують аспекти державної та приватної хмар, дозволяючи організаціям контролювати свої дані та ресурси більше, ніж у загальнодоступному хмарному середовищі, але все одно організацію можуть скористатися масштабованістю та іншими перевагами публічної хмари, коли це необхідно.

Постачальники хмарних послуг розглядають проблеми та ризики хмарної безпеки як спільну відповідальність. У цій моделі постачальник хмарних послуг покриває безпеку самої хмари, а клієнт - безпеку того, що вони в неї вкладають. У кожній хмарній службі - від програмного забезпечення як послуги (SaaS), як Microsoft Office 365, до інфраструктури як послуги (IaaS), як Amazon Web Services (AWS), клієнт хмарних обчислень завжди відповідає за захист своїх даних від загроз безпеці та контролю доступу до них. На рисунку представлено, як поділяється безпека між клієнтом та постачальником згідно сервісу, який вони отримують.

Інфраструктура як послуга (IaaS)

Вмикає модель на вимогу для попередньо налаштованих віртуальних обчислювальних ресурсів центру обробки даних (тобто мережі, сховища та операційних систем). Це може включати автоматизацію створення віртуальних машин у масштабі, тому дуже важливо врахувати, як віртуальні машини забезпечуються, управляються та працюють.

Платформа як послуга (PaaS)

Надає інструменти та іншу обчислювальну інфраструктуру, що дозволяє організаціям зосередитись на створенні та запуску веб-додатків та послуг. Середовища PaaS в основному підтримують розробників, операції та команди DevOps. Тут управління та налаштування прав та привілеїв самообслуговування є ключовим для контролю ризику.

Програмне забезпечення як послуга (SaaS)

Складається з додатків, розміщених третьою стороною та зазвичай наданих як програмні послуги через веб-браузер, доступ до якого здійснюється на стороні клієнта. Хоча SaaS позбавляє потреби розгортати та керувати програмами на пристроях кінцевих користувачів, потенційно будь-який співробітник може отримати доступ до веб-служб та завантажувати вміст. Таким чином, необхідний належний контроль за видимістю та доступом для моніторингу типів доступних програм SaaS, їх використання та вартості, як це показано на рисунку 1.4.

Shared Responsibility Model for Security in the Cloud

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility — Cloud Provider Responsibility

Рис.1.4 – Зони відповідальності користувача та хмарного провайдера

Більшість ризиків безпеки хмарних обчислень пов'язані з безпекою хмарних даних. Незалежно від недостатньої видимості даних, неможливості контролювати дані чи крадіжки даних у хмарі, більшість проблем торкаються даних, які клієнти розміщують у хмарі.

1.3.1. Переваги хмарних сховищ

Люди обирають хмару на противагу звичайній інфраструктурі з декількох причин. Те, як показує практика, до найголовніших переваг хмар варто віднести:

1. Здатність швидко і легко змінюватись;

Оскільки можна створити щось, працювати з цим, і коли даний продукти стане непотрібен можна видалити його. Наприклад, коли потрібно створити сотні віртуальних машин, щоб щось протестувати, в хмарі це робиться значно швидше, просто скориставшись консоллю. Разом з автоматизацією це дає велику силу, розглянемо для прикладу ситуацію, коли потрібно створити п’ять сотень груп безпеки в декількох регіонах одного сервісу і максимально збільшити права кожної групи, щоб провести один тест, а по закінченню все видалити, і це справді та мобільність, яку отримуємо використовуючи хмару.

2. Стійкість;

Хмара насправді є менш стійкою, будь-яка віртуальна машина є менш стійкою ніж добре сконфігуроване фізичне обладнання, але, провайдери добре усвідомлені про цей недолік, і хмарні сховища наділені вбудованою відмовостійкостю, тому, коли потрібно зберегти файл в віртуальному сховищі, фрагменти цього файлу зберігаються в п’яти чи десяти різних місцях, що автоматично робить хмарні сховища більш відмовостійкими.

3. Автоматичне оновлення програмного забезпечення

Немає нічого більш дратуючого, ніж те, що потрібно чекати встановлення оновлень системи. Хмарні програми автоматично оновлюються та оновлюються самостійно, замість того, щоб змушувати IT-відділ виконувати оновлення, що здійснюється вручну в масштабі всієї організації. Це економить дорогоцінний IT-персонал і гроші, витрачені на зовнішні IT-консультації. PCWorld перелічує, що

50% хмарних розробників зазначили, як хмарну перевагу те, що потрібно менше внутрішніх IT-ресурсів.

4. Економічна вигода;

Економічна вигода полягає в тому, що ви платите за те, чим користуєтесь, і вам не доведеться переплачувати. Опинившись у хмарі, легкий доступ до даних вашої компанії заощадить час і гроші на запуск проектів. А для тих, хто переживає, що в кінцевому підсумку вони заплатять за функції, які їм не потрібні, то за більшість послуг хмарних обчислень користувачі платять у міру необхідності. Це означає, що якщо ви не корисутуєтеся тим, що пропонує хмара, то, принаймні, вам не доведеться витрачати на це гроші.

Система оплати за використання також застосовується до місця зберігання даних, необхідного для обслуговування зацікавлених сторін та клієнтів, а це означає, що ви отримаєте рівно стільки місця, скільки вам потрібно, і за вас не стягуватиметься плата за простір, що вам не потрібен. У сукупності ці фактори призводять до зниження витрат і більшої віддачі.

5. Екологічний аспект;

Враховуючи поточний стан навколишнього середовища, організаціям вже недостатньо розміщувати сміттєвий контейнер у прибиральні та стверджувати, що вони роблять свою справу, щоб допомогти планеті. Справжня екологічність вимагає рішень, що стосуються марнотратства на кожному рівні бізнесу. Хостинг на хмарі є більш екологічним та зменшує вуглецевий слід.

Хмарні інфраструктури підтримують екологічну активність, забезпечуючи віртуальні послуги, а не фізичні продукти та обладнання, і скорочуючи паперові відходи, покращуючи енергоефективність та (враховуючи, що це дозволяє працівникам доступ з будь-якого місця з підключенням до Інтернету), зменшуючи викиди, пов'язані з поїздками. У звіті Pike Research передбачається, що споживання енергії в центрі обробки даних зменшиться на 31% з 2010 по 2020 рік на основі прийняття хмарних обчислень та інших варіантів віртуальних даних.

6. Безпека

Багато організацій турбуються про безпеку, коли йдеться про прийняття рішення щодо переходу до хмарних обчислень. Зрештою, коли файли, програми та інші дані не надійно зберігаються на місці, як ви можете знати, що вони захищені? Якщо ви можете віддалено отримати доступ до своїх даних, то що заважає кіберзлочинцю робити те саме? Саме ці запитання турбують підприємців. З одного боку, штатна робота хмарного хоста полягає в ретельному відстеженні безпеки, що значно ефективніше, ніж у звичайній внутрішній системі, коли організація повинна розподілити свої зусилля між безліччю IT-проблем, причому безпека є лише однією з них. І хоча більшість підприємств не люблять відкрито розглядати можливість внутрішнього викрадення даних, правда полягає в тому, що надзвичайно високий відсоток крадіжок даних відбувається внутрішньо і здійснюється працівниками. Коли це так, насправді може бути набагато безпечніше зберігати конфіденційну інформацію за межами сайту. Звичайно, все це дуже абстрактно, тому давайте розглянемо статистику. RapidScale стверджує, що 94% підприємств побачили поліпшення безпеки після переходу на хмару, а 91% заявили, що хмара полегшує відповідність вимогам уряду. Ключем до цієї посиленої безпеки є шифрування даних, що передаються через мережі та зберігаються в базах даних. Використовуючи шифрування, інформація стає менш доступною для хакерів або тих, хто не має дозволу переглядати ваші дані. Як додатковий захід безпеки, у більшості хмарних служб можна встановити різні параметри безпеки залежно від користувача.

1.3.1. Безпека SaaS

Не зважаючи на всі переваги хмарних сховищ, як і будь-яке рішення, воно має свої недоліки та прогалини в безпеці, розглянемо найчастіше згадувані проблеми відповідно до типу сервісу, що надається провайдером. Найважливіші питання безпеки SaaS у хмарі:

1. Відсутність видимості даних про хмарні програми
2. Викрадення даних із хмарного додатка зловмисником

3. Неповний контроль над тим, хто може отримати доступ до конфіденційних даних

4. Неможливість моніторингу даних під час передачі до хмарних додатків та назад

5. Хмарні програми, що надаються поза межами видимості IT (наприклад, тіньові IT)

6. Відсутність персоналу, який володіє навичками управління безпекою хмарних додатків

7. Неможливість запобігти зловмисному розкраданню інсайдерів або неправильному використанню даних

8. Розширені загрози та атаки на постачальника хмарних додатків

9. Неможливість оцінити безпеку операцій постачальника хмарних додатків

10. Неможливість підтримувати відповідність нормативним актам.

Проблеми безпеки хмарної безпеки SaaS, природно, зосереджені на даних та доступі, оскільки більшість моделей спільної відповідальності за безпеку залишають ці два питання єдиною відповідальністю для клієнтів SaaS. Кожна організація несе відповідальність за розуміння того, які дані вони розміщують у хмарі, хто може до них отримати доступ та який рівень захисту вони (та постачальник хмарних служб) застосовують.

Важливо також врахувати роль постачальника послуг SaaS як потенційної точки доступу до даних та процесів організації. Такі розробки, як XcodeGhost та програми-вимагачі GoldenEye, підкреслюють, що зловмисники визнають цінність постачальників програмного забезпечення та хмарних послуг як вектора для атаки на більші активи. В результаті зловмисники все більше зосереджуються на цій потенційній вразливості.

1.3.2. Безпека IaaS

До найважливіших питань безпеки IaaS у хмарі відносяться:

1. Хмарні робочі навантаження створюються поза видимістю.
2. Неповний контроль над конфіденційними даними.

3. Викрадення даних, розміщених у хмарній інфраструктурі зловмисником.
4. Брак персоналу, який володіє навичками захисту хмарної інфраструктури.
5. Відсутність видимості даних у хмарі.
6. Неможливість запобігти зловмисному розкраданню інсайдерів.
7. Відсутність послідовних засобів контролю над середовищами.
8. Розширені загрози та атаки на хмарну інфраструктуру.
9. Неможливість контролю хмарних систем на наявність вразливостей
10. Побічне поширення атаки з одного навантаження хмари на інше.

Захист даних є критично важливим для IaaS. Оскільки відповідальність клієнта поширюється на програми, мережевий трафік та операційні системи, з'являються додаткові загрози. Організаціям слід розглянути останній розвиток атак, які виходять за межі даних, як центр ризику IaaS.

Створюючи інфраструктуру в хмарі, важливо оцінити свою здатність запобігати крадіжці та контролювати доступ. Визначення того, хто може вводити дані в хмару, відстеження модифікацій ресурсів для виявлення ненормальної поведінки, засоби захисту та зміцнення інструментів оркестрації, а також додавання мережевого аналізу трафіку північ-південь та схід-захід як потенційний сигнал компромісу - все це швидко стає стандартним заходом у захист розгортання хмарної інфраструктури в масштабі.

1.3.3. Безпека Private Cloud

До найважливіших проблем безпеки приватних хмар відносяться:

1. Відсутність послідовних засобів контролю, що охоплюють традиційні серверні та віртуалізовані приватні хмарні інфраструктури
2. Збільшення складності інфраструктури, що призводить до збільшення часу / зусиль для впровадження та обслуговування
3. Брак персоналу, який володіє навичками управління безпекою програмно визначеного центру обробки даних (наприклад, віртуальних обчислень, мережі, сховища)

4. Неповна видимість безпеки для програмно визначеного центру обробки даних (наприклад, віртуальних обчислень, мережі, сховища)
5. Розширені загрози та атаки

Важливим фактором у процесі прийняття рішень щодо розподілу ресурсів між державною та приватною хмарою є тонко налаштований контроль, доступний у приватних хмарних середовищах. У приватних хмарах додаткові рівні контролю та додатковий захист можуть компенсувати інші обмеження розгортання приватної хмари та можуть сприяти практичному переходу від монолітних серверних центрів обробки даних.

У той же час організації повинні враховувати, що підтримка тонко налаштованого контролю створює складність, принаймні за межі того, в що перетворилася публічна хмара. В даний час хмарні провайдери докладають багато зусиль, щоб самостійно підтримувати інфраструктуру. Користувачі хмарних служб можуть спростити управління безпекою та зменшити складність завдяки абстрагуванню елементів управління. Це об'єднує загальнодоступні та приватні хмарні платформи над фізичними, віртуальними та гібридними середовищами.

Як бачимо, проаналізувавши все сказане вище, можемо зауважити, що проблеми не сильно різняться від сервісу до сервісу, наприклад проблеми з видимістю даних чи інсайдерами, проте існують варіанти боротьби з цими недоліками, які реалізуються в практичній частині.

1.4. Найрозповсюдженіші атаки

Розглянемо детальніше загальні типи атак притаманні всім сервісам.

Витік даних

Витік даних - це інцидент в галузі кібербезпеки, де конфіденційна інформація оприлюднена, переглянута, викрадена або використана несанкціонованою особою. Порушення даних може бути основною метою цілеспрямованої атаки або просто результат людської помилки, застосування вразливостей або неадекватні практики безпеки. Витік даних включає будь-яку інформацію, яка не була призначена для загального користування, включаючи, але не обмежуючись цим, особисту

інформацію про здоров'я, фінансову інформацію, інформація, що ідентифікує особу (ІПІ) та інтелектуальна власність.

Негативні наслідки порушення даних можуть включати:

1. Вплив на репутацію та довіру клієнтів чи партнерів

2. Втрата інтелектуальної власності (ІВ) конкурентам

3. Нормативні наслідки, які можуть призвести до грошових втрат

4. Вплив на бренд, який може спричинити зниження ринкової вартості

5. Юридичні та договірні зобов'язання

6. Фінансові витрати, понесені внаслідок реагування на події та судово-медичної експертизи

Неправильна конфігурація та неадекватний контроль змін

Неправильна конфігурація виникає, коли обчислювальні ресурси налаштовані неправильно, часто роблячи їх вразливими до зловмисної діяльності.

Деякі загальні приклади включають:

• Незахищені елементи зберігання даних або контейнери

• Надмірні дозволи

• Вхідні дані за замовчуванням та налаштування конфігурації залишаються без змін

• Вимкнено стандартний контроль безпеки

Неправильна конфігурація хмарних ресурсів є основною причиною порушення даних і може дозволити видалення або зміну ресурсів та переривання обслуговування.

Відсутність ефективного контролю змін є поширеною причиною неправильної конфігурації в хмарному середовищі. Хмарні середовища та методології хмарних обчислень відрізняються від традиційних інформаційних технологій (ІТ) тим, що ускладнює контроль за змінами. Традиційні процеси змін включали безліч ролей та схвалень, і для досягнення фази виробництва могли знадобитися дні чи тижні. Елементи інфраструктури, які були статичними в корпоративному центрі обробки даних, тепер абстрагуються до програмного забезпечення в хмарі, і весь їх життєвий цикл може тривати лише кілька хвилин або секунд. Методи хмарних обчислень

покладаються на автоматизацію, розширення ролей та доступ для підтримки швидких змін.

Використання декількох хмарних провайдерів додає складності, оскільки кожен провайдер має унікальні можливості, які розширюються майже щодня. Це динамічне середовище вимагає гнучкого та активного підходу до контролю та виправлення змін, який багато компаній ще не засвоїли.

Відсутність архітектури та стратегії хмарної безпеки

В усьому світі організації переносять частину своєї IT-інфраструктури в загальнодоступні хмари. Однією з найбільших проблем під час цього переходу є впровадження відповідної архітектури безпеки для протидії кібератакам. На жаль, цей процес залишається загадкою для багатьох організацій. Дані піддаються різним загрозам, коли організації припускають, що міграція в хмару - це спроба простого перенесення існуючого IT-стека та засобів контролю в хмарне середовище. Відсутність розуміння моделі спільної відповідальності за безпеку також є ще одним фактором, що сприяє цьому.

Крім того, функціональність та швидкість міграції часто мають перевагу над безпекою. Ці фактори призводять до відсутності архітектури та стратегії безпеки в хмарі, що робить організації вразливими до успішних кібератак. Впровадження відповідної архітектури безпеки та розробка надійної стратегії безпеки нададуть організаціям міцну основу для роботи та ведення ділової діяльності в хмарі. Використання власних хмарних інструментів для підвищення видимості в хмарних середовищах також мінімізує ризик та витрати. Такі застережні заходи, якщо їх вжити, значно зменшать ризик компроментації.

Незалежно від того, наскільки великим чи малим є підприємство, правильна архітектура та стратегія безпеки є необхідними елементами для безпечного переміщення, розгортання та роботи в хмарі. Успішні кібератаки можуть мати серйозні наслідки для бізнесу, включаючи фінансові втрати, шкоду репутації, юридичні наслідки та штрафи.

Превентивні межі:

1. Забезпечити відповідність архітектури безпеки бізнес-цілям та завданням.

2. Розробити та впровадити структуру архітектури безпеки.

3. Забезпечте постійне оновлення моделей загроз.

4. Включити постійний моніторинг у загальну позицію безпеки.

Недостатня кількість ідентифікаційних даних, облікових даних, доступу та управління ключами

Системи управління ідентифікацією, обліковими даними, доступом включають інструменти та політики, що дозволяють організаціям керувати, контролювати та забезпечувати доступ до цінних ресурсів. Приклади можуть складатися з електронних файлів, комп'ютерних систем та фізичних ресурсів, таких як серверні кімнати та будівлі.

Хмарні обчислення вносять численні зміни до традиційних практик внутрішнього управління системою, пов'язаних з управлінням ідентифікацією та доступом (IAM). Це не те, що це обов'язково нові проблеми. Швидше, вони є більш важливими проблемами при роботі з хмарою, оскільки хмарні обчислення глибоко впливають на ідентичність, облікові дані та управління доступом. Як у загальнодоступних, так і в приватних хмарних налаштуваннях, CSP і споживачі хмарних служб повинні керувати IAM без шкоди для безпеки.

Інциденти з безпекою та порушення даних можуть статися через наступне:

• Недостатній захист посвідчень

• Відсутність регулярного автоматизованого обертання криптографічних ключів, паролів та сертифікатів

• Відсутність масштабованих систем управління ідентифікацією, обліковими даними та доступом

• Невикористання багатофакторної автентифікації

• Невикористання надійних паролів

Повноваження та криптографічні ключі не можна вбудовувати у вихідний код або розповсюджувати у відкритих сховищах (таких як GitHub), оскільки існує великий ризик виявлення та неправильного використання. Ключі повинні бути належним чином захищені за допомогою добре захищеної інфраструктури відкритих ключів (PKI), щоб забезпечити проведення заходів з управління ключами.

Системи управління особами повинні масштабуватися, щоб керувати життєвим циклом для мільйонів користувачів, а також CSP. Системи управління особами повинні підтримувати негайне припинення доступу до ресурсів із змінами персоналу, такими як припинення роботи або перехід на роботу. Такі процеси життєвого циклу управління ідентифікацією повинні бути інтегровані та автоматизовані в хмарних середовищах і здійснюватися своєчасно.

Системи ідентичності стають дедалі взаємопов'язаними. Об'єднання ідентичності з хмарним постачальником (наприклад, мовою розмітки тверджень безпеки (SAML)) стає все більш поширеним, щоб полегшити тягар обслуговування користувачів. Організації, які планують об'єднати ідентичність із хмарним провайдером, повинні розуміти безпеку навколо рішення ідентифікації хмарного провайдера, включаючи процеси, інфраструктуру та сегментацію між клієнтами (у випадку спільного рішення ідентифікації).

Найкращі практики вимагають багатофакторних систем автентифікації - смарт-картки, одноразового пароля (OTP) та автентифікації телефону, наприклад, для привілейованих користувачів та операторів хмарних послуг (тобто хмарного клієнта). Ці форми автентифікації допомагають вирішити питання викрадення паролів, коли викрадені паролі забезпечують доступ до ресурсів без згоди користувача.

У випадках, коли застарілі системи вимагають використання лише паролів, система автентифікації повинна підтримувати дотримання правил, таких як перевірка надійних паролів та визначені організацією політики періоду ротації.

Управління криптографічними ключами, що використовуються для захисту даних у стані спокою, має відбуватися протягом усього їх життєвого циклу, включаючи створення, розповсюдження, зберігання, заміну та видалення. Це допомагає розв'язувати атаки, які передбачають несанкціонований доступ до ключів. Викрадені криптографічні ключі - в поєднанні з відсутністю політики ротації ключів - можуть різко збільшити фактичний час та обсяг ефективного порушення. Будь-який централізований механізм зберігання, що містить секрети даних (наприклад, паролі, приватні ключі або конфіденційні бази даних контактів із

клієнтами), є цільовою метою для зловмисників. Вибір централізації паролів і ключів є компромісом, який організація повинна ретельно продумати: зручність централізованого управління ключами проти загрози групування цих ключів. Як і у випадку з будь-яким цінним активом, моніторинг та захист ідентичності та системи управління ключами повинні бути пріоритетними.

Зловмисні особи, що видаються законними користувачами, операторами або розробниками, можуть:

• Читати, вилучати, змінювати та видаляти дані

• Видати площину управління та функції управління

• Переглядати дані під час передачі

Випуск шкідливого програмного забезпечення, яке, здається, походить із законного джерела. Як результат, недостатня кількість ідентифікаційних даних, облікових даних або управління ключами може забезпечити несанкціонований доступ до даних та потенційно катастрофічну шкоду для організацій або кінцевих користувачів.

Превентивні методи:

1. Захист облікових записів, включаючи двофакторну автентифікацію та обмеження використання кореневих облікових записів.

2. Практика найсуворіших засобів контролю ідентичності та доступу для хмарних користувачів та ідентифікацій.

3. Виділення та сегментація рахунків, віртуальних приватних хмар (VPC) та груп ідентифікаційних даних щодо потреб бізнесу та принципу найменших привілеїв.

4. Поверніть ключі, видаліть невикористані облікові дані або привілеї доступу та використовуйте центральне програмне управління ключами.

Викрадення облікового запису

Викрадення облікового запису - це загроза, в якій зловмисники отримують доступ до облікових записів, які є надзвичайно привілейованими та конфіденційними. У хмарних середовищах обліковими записами з найбільшим ризиком є облікові записи хмарних служб або підписки. Фішинг-атаки,

використання хмарних систем або викрадені облікові дані можуть скомпрометувати ці облікові записи. Ці унікальні та потенційно потужні загрози можуть спричинити значні порушення хмарного середовища, такі як втрата даних та активів та скомпрометовані операції. Ці ризики випливають із моделі доставки хмарних служб, а також моделі її організації та управління: дані та програми знаходяться в хмарних послугах, які знаходяться в хмарному обліковому записі або підписці. Підписки, зокрема, доступні в Інтернеті кожному, хто має привілеї та повноваження.

Організації повинні енергійно пропагувати обізнаність про ці загрози та стратегії поглибленого захисту, щоб стримувати збитки від порушень.

Наслідки викрадення облікового запису включають витік даних, що призводить до шкоди репутації, погіршення вартості торгової марки, викриття юридичної відповідальності та розкриття конфіденційної особистої та ділової інформації.

Інсайдерська загроза

Команда комп'ютерних служб реагування на надзвичайні ситуації (CERT) Карнегі Меллона визначає інсайдерську загрозу як «потенційну можливість особи, яка має або дозволила доступ до активів організації, використовувати їхній доступ, зловмисно чи ненавмисно, діяти таким чином, що може негативно вплинути на організацію». Інсайдери можуть бути нинішніми чи колишніми працівниками, підрядниками чи іншими довіреними діловими партнерами. На відміну від зовнішніх правопорушників, інсайдери не повинні проникати через брандмауери, віртуальні приватні мережі (VPN) та інші засоби захисту периметра. Інсайдери працюють у колі довіри компанії, де вони мають прямий доступ до мереж, комп'ютерних систем та конфіденційних даних компанії. Інсайдерські загрози є більш поширеними, ніж ви можете подумати. Звіт Netwrix 2018 Cloud Security вказує, що 58 відсотків компаній приписують порушення безпеки інсайдерам.

Недбалість співробітників або підрядника була основною причиною 64 відсотків повідомлених інцидентів з інсайдерською діяльністю, тоді як 23 відсотки були пов'язані з інсайдерами, що вчинили злочин, та 13 відсотків - з викраденням вірогідних даних, згідно з дослідженням Інституту Понемона за 2018 рік. Деякі

поширені сценарії включають неправильно налаштовані хмарні сервери, співробітники, що зберігають конфіденційні дані компанії на власних незахищених персональних пристроях та системах, а також співробітники та інші інсайдери, які стають жертвами фішинг-листів, що призвели до зловмисних атак на активи компанії.

Превентивні межі:

Вжиття заходів для мінімізації недбалості з боку інсайдерів може допомогти пом'якшити наслідки внутрішніх загроз. Дії, описані нижче, можуть допомогти вирішити проблеми безпеки, спричинені недбалими користувачами та адміністраторами.

1. Навчання та освіта співробітників служб безпеки: Проведіть тренінг для своїх команд безпеки, як правильно встановлювати, налаштовувати та контролювати комп’ютерні системи, мережі, мобільні пристрої та резервні пристрої.

2. Регулярне підвищення кваліфікації працівників: Проведіть навчання для своїх постійних співробітників, щоб проінформувати їх, як боротися з ризиками безпеки, такими як фішинг та захист корпоративних даних, які вони несуть за межами компанії на ноутбуках та мобільних пристроях. Вимагайте використання надійних паролів і частого оновлення паролів. Повідомте працівників про наслідки, пов’язані із здійсненням зловмисної діяльності.

3. Виправлення неправильно налаштованих хмарних серверів: регулярно перевіряйте сервери в хмарі та локально, а потім виправляйте будь-які відхилення від безпечного базового рівня, встановленого в організації.

4. Обмежте доступ до критично важливих систем: Переконайтесь, що привілейований доступ до систем безпеки та центральних серверів обмежується мінімальною кількістю співробітників, і що ці особи включають лише тих, хто пройшов навчання з управління адмініструванням критично важливих комп'ютерних серверів. Контролюйте доступ до всіх комп'ютерних серверів на будь-якому рівні привілеїв.

Небезпечні інтерфейси та API

Постачальники хмарних обчислень надають набір програмних інтерфейсів користувача (UI) та API, що дозволяє клієнтам керувати хмарними службами та взаємодіяти з ними. Безпека та доступність загальних хмарних служб залежать від безпеки цих API.

Від аутентифікації та контролю доступу до шифрування та моніторингу активності, ці інтерфейси повинні бути розроблені для захисту як від випадкових, так і від зловмисних спроб обійти політику безпеки.

Погано розроблені API можуть призвести до неправильного використання або, що ще гірше, до порушення даних. Поламані, викриті або зламані API спричинили деякі серйозні порушення даних. Організації повинні розуміти вимоги безпеки щодо проектування та представлення цих інтерфейсів в Інтернеті.

API та користувацькі інтерфейси, як правило, є найбільш відкритими частинами системи, можливо, єдиним активом із загальнодоступною IP-адресою, доступною поза межами довіреної організації. Як «вхідні двері» на них, з великою ймовірністю, постійно здійснюватимуться напади; отже, необхідна захищена конструкція та належний контроль, що захищає їх від атак.

Превентивні межі:

1. Практикуйте належну гігієну API. Належна практика включає ретельний нагляд за такими предметами, як інвентар, випробування, аудит та захист від ненормальної діяльності.
2. Забезпечте належний захист ключів API та уникайте повторного використання.
3. Подумайте про використання стандартних та відкритих фреймворків API (наприклад, Open Cloud Computing Interface (OCCI) та Cloud Infrastructure Management Interface (CIMI)).

Помилки метаструктури та списку додатків

Постачальники хмарних послуг регулярно розкривають операції та засоби захисту, необхідні для успішного впровадження та захисту своїх систем. Зазвичай виклики API розкривають цю інформацію, а захист вбудований у рівень

метаструктури для CSP. Метаструктура вважається лінією демаркації CSP / замовника - також відомою як ватерлінія.

У цій моделі можливості відмов існують на декількох рівнях. Наприклад, погана реалізація API CSP пропонує зловмисникам можливість заважати хмарним клієнтам, перериваючи конфіденційність, цілісність або доступність послуги.

Щоб покращити видимість хмар для клієнтів, CSP часто виявляли або дозволяли взаємодію API із процесами безпеки на ватерлінії. Незрілі CSP часто не впевнені в тому, як зробити API доступними для своїх клієнтів - і в якій мірі. Наприклад, API, які дозволяють клієнтам отримувати журнали або перевіряти доступ до системи, можуть містити дуже конфіденційну інформацію. Однак цей процес також необхідний орендарям для виявлення несанкціонованого доступу. Над ватерлінією споживачі хмар повинні розуміти, як правильно впровадити хмарні програми для повного використання хмарної платформи. Наприклад, програми, не розроблені для хмарних середовищ, не зможуть повноцінно взаємодіяти та використовувати наявні хмарні ресурси та можливості. Простого підходу "підняти-змінити" недостатньо при перенесенні ділових операцій та додатків у хмару.

Превентивні межі:

1. Постачальники хмарних послуг повинні пропонувати видимість та викривати пом’якшувальні дії, щоб протидіяти властивій хмарі недостатній прозорості для орендарів.

2. Орендарі хмарних служб повинні впроваджувати відповідні функції та засоби керування у власному дизайні хмар.

3. Усі CSP повинні проводити тестування на проникнення та надавати висновки клієнтам.

Обмежена видимість використання хмари

Обмежена видимість використання хмари виникає, коли організація не має можливості візуалізувати та аналізувати безпечне чи шкідливе використання хмарних служб в організації. Ця концепція розбита на дві ключові проблеми. Несанкціоноване використання додатків: Це відбувається, коли працівники використовують хмарні програми та ресурси без спеціального дозволу та підтримки

корпоративних IT та безпеки. Результатом цього сценарію є модель самопідтримки під назвою Shadow IT. Коли незахищена діяльність хмарних служб не відповідає корпоративним вимогам, така поведінка є ризикованою - особливо у поєднанні з чутливими корпоративними даними. Гартнер прогнозує, що до 2021 року третина всіх успішних атак безпеки на компанії відбуватиметься через тіньові IT-системи та ресурси.

Зловживання санкційними програмами: організації часто не можуть проаналізувати, як інсайдери, які використовують санкційну програму, використовують їх затверджені програми. Часто це використання відбувається без явного дозволу компанії або сторонніх акторів загроз, які націлюють службу за допомогою таких методів, як викрадення облікових даних, введення структуризованої мови запитів (SQL), атаки на систему доменних імен (DNS) тощо. У більшості випадків зводиться до розрізнення дійсних та недійсних користувачів між собою шляхом визначення того, чи їх поведінка не відповідає нормам, чи вони дотримуються корпоративної політики.

Превентивні межі:

Пом'якшення цих ризиків починається з розробки повних зусиль щодо видимості хмар зверху вниз. Цей процес, як правило, бере початок із доручення архітектора хмарної безпеки організації створенням комплексного рішення, яке пов’язує людей, процеси та технології. Дії, описані нижче, можуть допомогти розпочати цей процес.

1. Запропонувати загальнонаціональний тренінг з прийнятих політик використання хмар та їх застосування.

2. Усі не затверджені хмарні служби повинні бути переглянуті та схвалені архітектором хмарної безпеки або стороннім управлінням ризиками.

3. Інвестуйте в такі рішення, як брокери безпеки хмарного доступу (CASB) або програмно визначені шлюзи (SDG), щоб проаналізувати вихідні дії та допомогти виявити використання хмари, користувачів, що перебувають під загрозою ризику, та відслідковувати використання поведінки уповноважених працівників для виявлення аномалій.

4. Інвестуйте у брандмауер веб-додатків (WAF), щоб проаналізувати всі вхідні підключення до ваших хмарних служб на наявність підозрілих тенденцій, зловмисного програмного забезпечення, розподіленого ризику відмови в обслуговуванні (DDoS) та ботнетів.

5. Виберіть рішення, спеціально розроблені для моніторингу та контролю всіх ключових хмарних додатків підприємства (планування корпоративних ресурсів, управління людським капіталом, комерційний досвід та управління ланцюгами поставок) та забезпечення подолання підозрілої поведінки.

6. Впроваджуйте модель нульової довіри у вашій організації.

1.5. Вимоги до постачальника хмарних послуг

Як вже було неодноразово сказано, питання безпеки покладаються як на клієнта так і на провайдера хмарних послуг. Як клієнт, щоб ваш бізнес відчував, що він може довіряти постачальнику хмарних послуг, вам слід розуміти, який тип захисту він запровадив. Починаючи оцінювати постачальника хмарних сховищ, слід оцінювати їх, виходячи з того, чи мають вони ключові заходи безпеки.

Перелік деяких найважливіших функцій безпеки, якими повинен володіти постачальник хмарних послуг наведений нижче:

Фізичні заходи

Перше, що потрібно встановити, - це чи є у постачальника хмарних послуг заходи фізичної безпеки. Якщо кіберзлочинці зможуть отримати фізичний доступ до приміщення постачальника хмарних сховищ, це може бути настільки ж шкідливим, як і кібератака.

Одне питання тут полягає у фізичному розташуванні серверів - чи пропонує провайдер центри обробки даних у різних місцях? Поширення даних по кількох центрах обробки даних - це чудовий спосіб мінімізувати ризик втрати або крадіжки даних.

У приміщеннях хмарних провайдерів також існує багато заходів фізичної безпеки, які повинна мати компанія, таких як відеоспостереження для цілодобового

нагляду та конкретні бар'єри для запобігання доступу автомобілів та швидкого проїзду.

Шифрування

Одним з основних напрямків захисту для будь-якого постачальника хмарних систем безпеки є шифрування. Хмара використовує складні алгоритми для приховування даних, що зберігаються в хмарі. Зашифровані дані марні і функціонально неможливо декодувати без ключа шифрування - через те, що це займе певний час та обчислювальні потужності, що зробить операцію безглуздою.

Шифрування даних розглядається як один з найважливіших заходів кібербезпеки, оскільки це означає, що навіть якщо ваші дані можуть бути використані злочинцями, вони не матимуть до них доступу і не зможуть їх використовувати будь-яким чином.

Шукайте постачальників хмарних послуг, які забезпечують локальне шифрування та дешифрування ваших файлів, а також пропонують резервне копіювання та зберігання. Це означає, що ваші дані повністю захищені на кожному кроці процесу.

Хмарні засоби контролю безпеки

Ваш постачальник хмарних послуг також повинен встановити низку засобів управління хмарною безпекою, щоб дані завжди були в безпеці. Існує багато різних типів засобів керування, тому вам потрібно, щоб постачальник розумів, які ключові заходи вони використовують. Деякі з найбільш важливих включають:

- Профілактичний контроль - хоча він не може усунути вразливості в системі, профілактичний контроль зміцнює систему в цілому. Вони можуть включати такі речі, як автентифікація для хмарних користувачів, що унеможливлює доступ неавторизованих користувачів до системи.
- Заходи стримування - вони ефективні для зменшення атак на систему, інформуючи потенційних зловмисників про потужні засоби захисту.
- Елементи контролю виявлення - ці засоби контролю виявляють і реагують на будь-які інциденти, що трапляються проти системи. Вони можуть включати моніторинг системи, мережі та кінцевої точки.

- Реактивні елементи управління - ці елементи управління намагаються обмежити збиток від атаки на систему. Наприклад, вони можуть відновити резервну копію системи, щоб її відновити у разі пошкодження.

Клієнти повинні вимагати прозорості, уникаючи постачальників, які відмовляються надавати детальну інформацію про програми безпеки. Задавати питання, що стосуються кваліфікації архітекторів, розробників та операторів; процеси управління ризиками та технічні механізми; і рівень тестування, яке було проведено для перевірки того, що процеси обслуговування та контролю функціонують належним чином, і що постачальники можуть ідентифікувати непередбачувані вразливості.

На додаток, ось сім конкретних питань безпеки, за якими, за словами Gartner, клієнти повинні звернутися до постачальників, перш ніж вибрати хмарного постачальника.

1. Пільговий доступ користувача. Конфіденційні дані, що обробляються за межами підприємства, несуть у собі власний рівень ризику, оскільки сторонні послуги обходять «фізичний, логічний та персональний контроль» IT-магазинів, які здійснюють внутрішні програми. Отримайте якомога більше інформації про людей, які керують вашими даними. "Попросіть постачальників надати конкретну інформацію щодо найму та нагляду за привілейованими адміністраторами та контролю над їх доступом", - говорить Гартнер.

2. Відповідність нормативним актам. Клієнти несуть відповідальність за безпеку та цілісність власних даних, навіть якщо вони зберігаються у постачальника послуг. Традиційні постачальники послуг проходять зовнішній аудит та сертифікацію безпеки. За словами Гартнера, постачальники хмарних обчислень, які відмовляються проходити такий контроль, "сигналізують, що клієнти можуть використовувати їх лише для найбільш тривіальних функцій".

3. Розташування даних. Коли ви використовуєте хмару, ви, мабуть, не будете точно знати, де розміщуються ваші дані. Насправді ви можете навіть не знати, в якій країні вони будуть зберігатися. Запитайте у постачальників, чи зобов’язуватимуться вони зберігати та обробляти дані у певних юрисдикціях, і чи прийматимуть вони

договірне зобов’язання виконувати місцеві вимоги щодо конфіденційності від імені своїх клієнтів, Радить Гартнер.

4. Розділення даних. Дані в хмарі, як правило, перебувають у спільному середовищі поряд із даними інших клієнтів. Шифрування є ефективним, але не є лікувальним засобом. "Дізнайтеся, що зроблено для розподілу даних у стані спокою", - радить Гартнер. Хмарний постачальник повинен надати докази того, що схеми шифрування були розроблені та перевірені досвідченими спеціалістами. "Нещасні випадки шифрування можуть зробити дані абсолютно непридатними для використання, і навіть звичайне шифрування може ускладнити доступність", - говорить Гартнер.

5. Одужання. Навіть якщо ви не знаєте, де знаходяться ваші дані, хмарний постачальник повинен повідомити вам, що станеться з вашими даними та послугою у випадку катастрофи. "Будь-яка пропозиція, яка не повторює дані та інфраструктуру додатків на кількох сайтах, є вразливою до повної відмови", - говорить Гартнер. Запитайте у свого постачальника, чи має він «можливість виконати повне відновлення та скільки часу це займе».

6. Слідче забезпечення. Розслідування неналежної або незаконної діяльності може бути неможливим у хмарних обчисленнях, попереджає Гартнер. «Хмарні служби особливо важко дослідити, оскільки ведення журналу та дані для кількох клієнтів можуть бути розташовані спільно, а також можуть бути розподілені між постійно мінливим набором хостів та центрів обробки даних. Якщо ви не можете отримати договірне зобов'язання на підтримку конкретних форм розслідування, а також доказів того, що постачальник вже успішно підтримав таку діяльність, тоді ваше єдине надійне припущення полягає в тому, що запити на розслідування та виявлення будуть неможливими ".

7. Довготривала життєздатність. В ідеалі ваш постачальник хмарних обчислень ніколи не впаде і його не поглине більша компанія. Але ви повинні бути впевнені, що ваші дані залишаться доступними навіть після такої події. «Запитайте потенційних постачальників»

1.6. Методи пом’якшення проблем безпеки хмарних обчислень

Ваша організація використовує хмарні служби, навіть якщо ці хмарні служби не є основною стратегією для ваших інформаційних технологій (IT). Для зменшення ризиків безпеки хмарних обчислень існує три найкращі практики, над якими повинні працювати всі організації.

По-перше, процеси DevSecOps - неодноразово демонструвалось, що DevOps та DevSecOps покращують якість коду та зменшують експлоїти та уразливості, а також збільшують швидкість розробки додатків та розгортання функцій. Інтеграція процесів розробки, контролю якості та безпеки в рамках бізнес-підрозділу чи команди програм - замість того, щоб покладатися на окрему групу перевірки безпеки - має вирішальне значення для роботи на швидкості сучасних вимог ділового середовища.

По-друге, автоматизовані інструменти розгортання та управління програмами - Дефіцит навичок безпеки в поєднанні зі збільшенням обсягу та темпу загроз безпеці означає, що навіть найдосвідченіший фахівець у галузі безпеки не може встигнути. Автоматизація, яка знімає буденні завдання та збільшує людські переваги за допомогою машинних переваг, є основною складовою сучасних IT-операцій.

По-третє, уніфікована безпека з централізованим управлінням усіма службами та постачальниками - Жоден продукт або постачальник не може доставити все, але безліч інструментів управління роблять занадто легким щось для проскакування. Єдина система управління з відкритою інтеграційною структурою зменшує складність, об’єднуючи деталі та впорядковуючи робочі процеси.

Нарешті, коли потрібно приймати рішення про компромісні рішення, краща видимість повинна бути пріоритетом №1, а не більшим контролем. Краще мати можливість бачити все в хмарі, ніж намагатися керувати неповною її частиною.

Висновки за розділом 1

Хмарні сховища - це надання розміщених послуг, включаючи як програмне, так і апаратне через Інтернет. Переваги швидкого розгортання, гнучкості, низьких початкових витрат та масштабованості зробили хмарні обчислення практично універсальними для організацій будь-якого розміру, часто як частина гібридної / багатохмарної архітектури інфраструктури та для звичайних користувачів. Хмарна безпека відноситься до технологій, політик, засобів управління та служб, які захищають хмарні дані, програми та інфраструктуру від загроз.

Жодна система не є досконалою, і це те саме для постачальників хмарних послуг. Однак, якщо ви оберете постачальника з потужними захисними засобами, ваш бізнес може скористатися багатьма перевагами безпеки використання хмари для зберігання ваших даних. Ви можете додатково пом'якшити будь-які ризики, запровадивши у своїй системі надійні процедури кібербезпеки та забезпечивши резервне копіювання всіх даних у разі найгіршого сценарію.

РОЗДІЛ 2
ОГЛЯД НЕОБХІДНИХ КОМПОНЕНТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ

2.1. Програмно-конфігурована мережа (SDN)

Програмно-конфігурована мережа є найбільшою різницею між хмарною та звичайною інфраструктурою.

Програмно-конфігурована мережа (SDN) - це архітектура, покликана зробити мережу більш гнучкою та простішою в управлінні. SDN централізує управління, абстрагуючи площину управління від функції пересилання даних у дискретних мережевих пристроях.

Архітектура SDN забезпечує централізовану програмовану мережу і складається з наступних елементів:

1. Контролер, основний елемент архітектури SDN, який забезпечує централізоване управління та контроль, автоматизацію та застосування політики у фізичному та віртуальному мережевих середовищах

2. API, які передають інформацію між контролером та окремими мережевими пристроями (такими як комутатори, точки доступу, маршрутизатори та брандмауери)

3. API наземного інтерфейсу, які передають інформацію між контролером та програмами та механізмами політики, для яких SDN виглядає як єдиний логічний мережевий пристрій.

SDN надає безліч переваг безпеки. По-перше, це сегрегація за замовчуванням, по-друге немає обмежень пов’язаних з фізичною топологією. По-третє, ніякого снифінгу, не зважаючи на те, що це віртуальні мережі, пакети йдуть прямолінійно від адресата до пункту призначення. По-четверте, може керувати безпечним маршрутом за допомогою тегів та абстракцій[2].

Всі великі хмарні платформи використовують SDN від приватних до публічних хмар.

Зупинимося на тому, як працює SDN, схема зображена на рисунку 2.1.

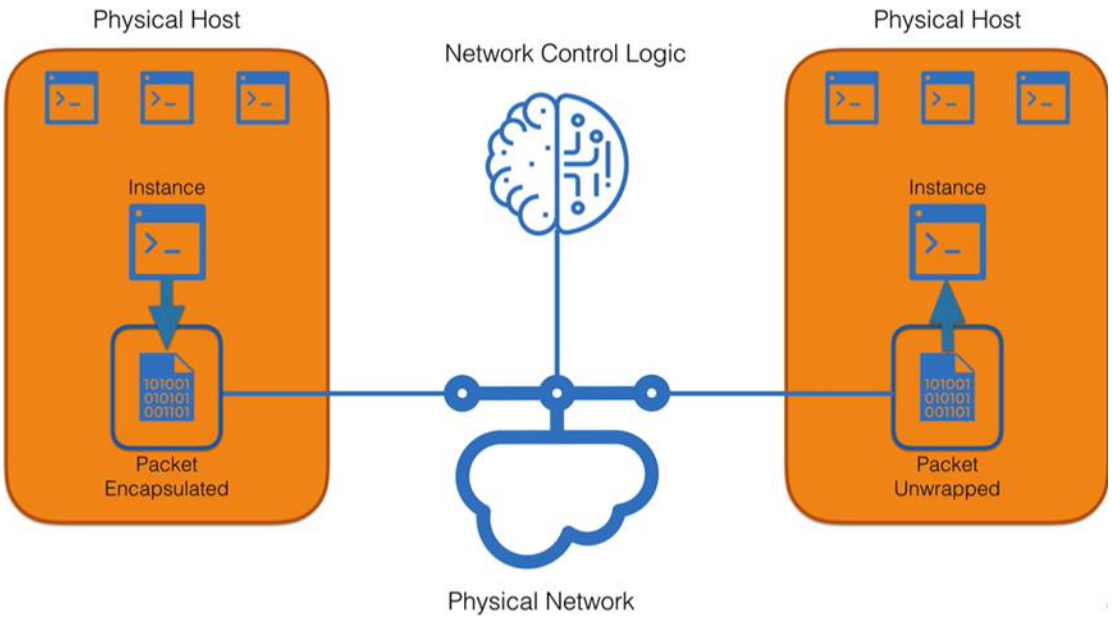

Рис.2.1 – Логічна схема роботи SDN

Для того, щоб все працювало залучена велика кількість протоколів, проте, якщо розглядати абстрактно, то все ще маємо фізичні сервера та фізичну мережу, ця віртуальна машина генерує пакет даних, який потрібно відправити, після цього він інкапсулюється, далі віртуальна машина додає інформацію про те, куди він має бути доставлений, після цього network control logic, вирішує куди відправити пакет, коли місце призначення досягнуто, пакет дикапсулюється.

Також SDN забезпечує різноманітні переваги безпеки. Клієнт може розділити мережеве з'єднання між кінцевим користувачем та центром обробки даних та мати різні налаштування безпеки для різних типів мережевого трафіку. Мережа може мати одну громадську мережу з низьким рівнем захисту, яка не стосується жодної конфіденційної інформації. Інший сегмент міг би мати набагато більш тонкий контроль віддаленого доступу із програмним забезпеченням брандмауера та політиками шифрування, які дозволяють пропускати через нього важливі дані[3-6].

Наприклад, якщо у клієнта є група IoT, він не відчуває, що все відповідає правилам з точки зору безпеки, за допомогою контролера SDN ви можете сегментувати цю групу подалі від критично важливого корпоративного трафіку.

Користувачі SDN можуть розгортати політики безпеки в мережі від центру обробки даних до краю, таке розгортання може бути на 30 - 60 відсотків дешевшим, ніж традиційне обладнання.

Можливість ознайомитися з набором робочих навантажень та визначити, чи відповідають вони певній політиці безпеки, є основною перевагою SDN, особливо при розподілі даних. Ще одним ключовим елементом безпеки, який дозволяє SDN, є можливість розгортання моделі безпеки" білого списку ", яка дозволяє лише певним об'єктам отримувати доступ до явних ресурсів у вашій мережеві.

За даними Casemore, все більша кількість платформ SDN зараз підтримує мікросегментацію. Насправді мікросегментація склалася як помітний варіант використання SDN. По мірі розширення платформ SDN для підтримки середовищ багатоголосного використання, вони будуть використовуватися для пом'якшення невід'ємної складності встановлення та підтримання послідовних політик мережі та безпеки на гібридних IT-ландшафтах[6-7].

2.2. Хмарні акаунти та радіус вибуху

Перше з чого слід почати побудову вашої хмарної інфраструктури – це звернути увагу на хмарні акаунти. Для мене це один з найкращих аспектів, щоб підкреслити переваги безпеки хмари перед традиційною інфраструктурою. В хмарі ви ніколи не бачите, що робить інший користувач. Це називається сегрегація, можливість відокремити ресурси та ізоляція, тобто можливість впевнитися в тому, що ті ресурси не бачать один одного. Сегрегація в хмарній інфраструктурі є абсолютною перевагою, оскільки забезпечити цей самий рівень відокремлення в фізичній інфраструктурі є досить затратно і часто громіздко. Також ізолювання мережі є важкою справою, оскільки це не лише сегрегація на канальному та транспортному рівнях, але й додаткове встановлення фаєрволів та DLP систем.

З іншого боку, з хмарою не потрібно думати про всі ці аспекти. Хмарні облікові записи схожі на окремі центри обробки даних і працюють дуже ефективно для стримування атак. Це є однією з найважливіших рекомендацій щодо хмарної

безпеки протягом багатьох років. Це також чудовий приклад використання хмари для переваг безпеки.

Вперше термін «радіус вибуху» був сказаний Шеннон Ліц на DevSecOps.org.

Ось концепція:

Облікові записи кожного хмарного провайдера повністю відокремлені та ізольовані один від одного. Це основна можливість багатостороннього управління. Це також те, що хмарний провайдер не може зіпсувати, якщо хоче продовжувати бізнес.

Ніщо не обмежує вас у придбанні кількох облікових записів у хмарного провайдера. Деякі хмарні провайдери дозволяють спілкуватися між обліковими записами. Зазвичай це досить обмежує, і обидві сторони повинні це налаштувати, і лише для дуже конкретних речей. Але ці «речі» можуть включати перехресне з'єднання мереж, міграцію сховища або спільне використання інших активів.

Облікові записи супер адміністратора (кореневі) різні для кожного облікового запису і не можуть бути пов'язані між собою.

Таким чином, ви можете використовувати облікові записи хмарних постачальників для розділення вашого середовища! Це серйозно обмежує радіус вибуху будь-яких подій безпеки, оскільки немає ніякого способу переходу між обліковими записами, крім тих конкретних підключень, які ви дозволяєте[7].

Використання кількох облікових записів, як і раніше, часто є найкращою практикою.

На даний момент рекомендується кілька облікових записів на проект для різних середовищ (наприклад, dev / test / prod / sec_monitoring). Це можна розглядати як спосіб обмежити діяльність адміністратора. Ви можете дозволити розробникам повний доступ адміністратора у своєму середовищі розробника, але заблокувати речі в тесті, а потім повністю заблокувати їх у виробництві. Методи DevOps можуть обробляти переміщення коду та оновлення в різних середовищах.

Деякі компанії мають сотні, якщо не тисячі, рахунків. Якщо трапляється щось погане, вони здувають весь акаунт і створюють його з нуля. Очевидно, що для цього потрібно використовувати автоматизацію та незмінну інфраструктуру.

Але подумайте про переваги. Кожен проект ізольований, будь-яке оточення ізольоване. Це робить майже неможливим для зловмисника рух в бік. Це робить мережеву сегрегацію видовищною.

Проте є й мінуси:

1. З такою інфраструктурою набагато складніше впоратися, оскільки немає централізації.
2. Потрібно абсолютно покладається на автоматизацію.
3. Потрібно бути дуже обережним з автоматизацією, щоб це не стало єдиною точкою відмови.
4. Не всі хмарні провайдери підтримують це.

На практиці є мало масштабних хмарних операцій, які з часом не закінчилися б таким підходом. Навіть більшість нових хмарних проектів у меншому масштабі починаються таким чином, виключно з експлуатаційних причин, якщо вони використовують будь-який тип безперервної доставки / розгортання (DevOps).

Роздивимося для прикладу, як це реалізовано в AWS, оскільки буде використовуватися саме цей хмарний провайдер на практиці.

Амазон має ієрархію, і насправді, більшість провайдерів також, в Azure це називається підписка, а в Google – проекти, де ви можете мати організаційні юніти які зв'язують всі ваші акаунти на логічному рівні, а потім ви можете це перенести на фізчний рівень, так щоб щоб це відповідало вашим вимогам щодо відповідності та доступності, як це зображено на рисунку 2.2[9].

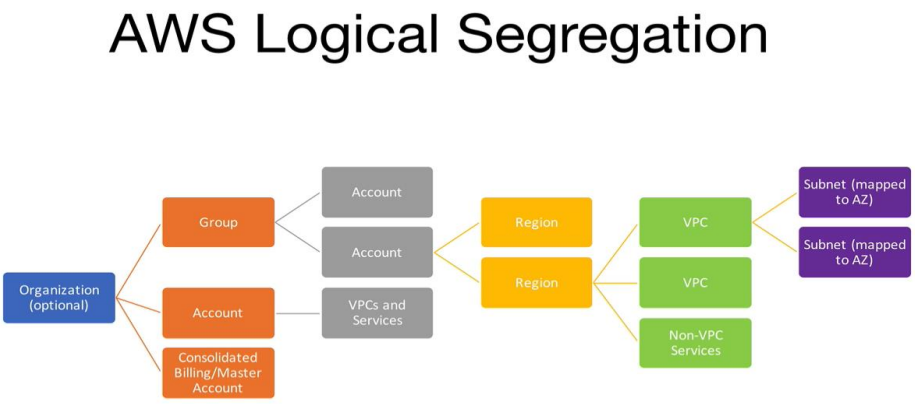

Рис.2.2 – Схема сегрегації в AWS

І з питань безпеки говоримо про використання цих інструментів для сегрегації, де можемо мати безліч акаунтів, різні регіони для відокремлення на фізичному рівні, далі це зони доступності та групи безпеки, як це зображено на рисунку 2.3.

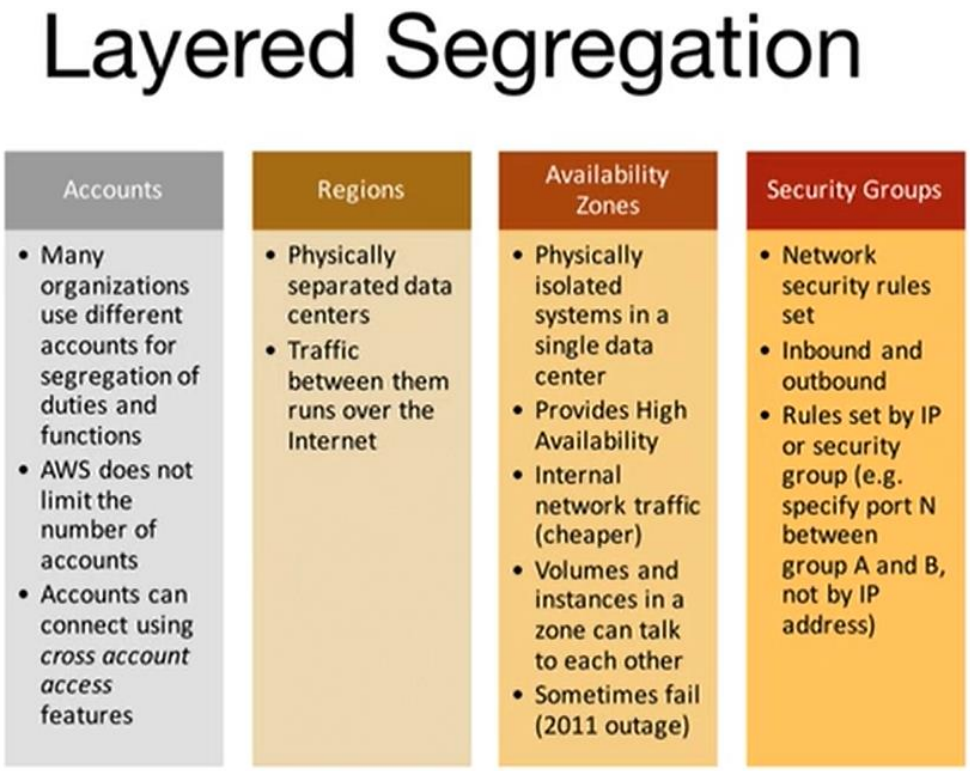

Рис.2.3 – Сегрегація по зонам

2.3. Групи безпеки

Група безпеки діє як віртуальний брандмауер для вашого екземпляра для контролю вхідного та вихідного трафіку. Коли ви запускаєте екземпляр у VPC, ви можете призначити екземпляру до п’яти груп безпеки. Групи безпеки діють на рівні екземпляра, а не на рівні підмережі. Отже, кожен екземпляр у підмережі у вашому VPC може бути призначений різному набору груп безпеки.

Для кожної групи безпеки ви додаєте правила, що контролюють вхідний трафік, до екземплярів та окремий набір правил, що контролюють вихідний трафік. Для управління вхідним та вихідним трафіком на кожному рівні можуть бути додані

різні правила. Правила схожі з тими правилами традиційних брандмауерів, де трафік може бути дозволений або заборонений на основі IP-адрес джерела або пункту призначення, протоколу, порту тощо.

Відмінності між групами безпеки та брандмауерами:

Групи безпеки - це важливий інструмент захисту ваших екземплярів від зовнішнього світу. Як і традиційні брандмауери, ви можете використовувати їх, щоб дозволити певному трафіку потрапляти до вашого екземпляра EC2, одночасно запобігаючи всім іншим. Але вони також мають деякі принципові відмінності від брандмауерів, перелічених нижче.

1. Ви не можете використовувати групи безпеки для явного блокування трафіку. Amazon дозволяє лише додавати правила дозвільного стилю, правила, які заперечують, не підтримуються. В основному забороняється весь вхідний трафік, якщо ви прямо цього не дозволите.
2. Правила можуть не посилатися на вихідні порти, підтримуються лише порти призначення.
3. За замовчуванням, коли ви вперше починаєте користуватися послугою EC2, AWS автоматично створює для вас групу безпеки та позначає її за замовчуванням. Він міститиме лише одне правило, яке дозволяє весь вхідний трафік через порт 22.
4. Поширеною практикою під час налаштування груп безпеки є фільтрація всього трафіку, використовуючи лише вхідні правила. Створені Групи безпеки містять правило, яке дозволяє всі вихідні підключення, а видалення цього правила також усуває нові вихідні підключення.
5. Варто зазначити, що групи безпеки мають державний статус, в яких зворотний трафік дозволяється автоматично; однак мережеві списки контролю доступу не мають стану, в яких зворотний трафік повинен бути чітко дозволений правилами. Це означає, що якщо ви замініте правило вихідного сигналу за замовчуванням, фільтруватимуться лише нові вихідні з'єднання. Будь-який вихідний трафік, який надсилається у відповідь на вхідне з'єднання, все одно буде дозволений.

6. Мережеві списки контролю доступу, на відміну від груп безпеки, не містять статусу та підтримують правила заборони. Це робить їх ідеальними для використання як додатковий рівень безпеки в будь-якому створеному VPC, особливо коли вам потрібно контролювати потік трафіку між підмережами.

2.4. Управління обліковими записами та доступом

Добре встановлено, що деякі традиційні парадигми IT-безпеки повинні бути переосмислені під час наближення власної безпеки в хмарі. Один із компонентів сильної позиції безпеки відіграє особливо важливу роль у хмарі - ідентичність. Поняття ідентичності в хмарі може стосуватися багатьох речей, але для цілей цього обговорення зупинимось на двох основних сутності: користувачах та хмарних ресурсах.

Історично склалося, що поглиблений захист здебільшого виконувався за допомогою елементів управління на рівні мережі. Удосконалені засоби запобігання загрозам здатні розпізнавати програми, які перетинають мережу, та визначати, чи слід їх дозволяти. Цей тип безпеки все ще дуже потрібен у середовищах, що перебувають у хмарі, але він сам по собі вже недостатній[8-11].

Державні хмарні провайдери пропонують багатий асортимент послуг, і єдиний спосіб керувати та захищати багато з них - це управління ідентифікацією та доступом (IAM).

IAM - це хмарний сервіс, який контролює дозволи та доступ для користувачів та хмарних ресурсів. Політики IAM - це набори політик дозволів, які можна приєднати або до користувачів, або до хмарних ресурсів, щоб визначити, до чого вони мають доступ і що з ним можна робити.

Поняття "ідентичність - це новий периметр" сягає ще часів 2012 року, коли AWS вперше оголосила про свою послугу IAM. Зараз знову спостерігаємо за зосередженням уваги на IAM через зростання абстрагованих хмарних служб та недавню хвилю гучних порушень даних.

Послуги, які не піддаються будь-якій базовій інфраструктурі, значною мірою покладаються на IAM для забезпечення безпеки. Наприклад, розглянемо програму,

яка слідує за цим потоком: тема "Проста служба сповіщень" (SNS) запускає функцію лямбда, яка, в свою чергу, поміщає елемент у таблицю DynamoDB. У цьому типі додатків немає мережі для перевірки, тому ідентифікація та дозволи стають найважливішими аспектами безпеки.

Як приклад впливу суворого (або надмірно дозволеного) профілю IAM, розглянемо конкретно функцію Лямбда. Функція повинна лише розміщувати елементи в таблиці DynamoDB. Що станеться, якщо функція скомпроментована з будь-якої причини, таблиця DynamoDB також одразу стає скомпроментованою, оскільки функція може використовуватися для вилучення даних.

Якщо профіль IAM дотримується принципу “найменших привілеїв” і дозволяє функції лише розміщувати елементи в таблиці, радіус вибуху значно зменшиться у випадку інциденту.

На практиці Федерація важлива, коли йдеться про ідентичність у хмарі. Федерація ідентичності - це метод, який використовує існуюче рішення для автентифікації, щоб надати доступ та авторизацію іншому рішенню, не відтворюючи ідентифікаторів користувачів.

Існує кілька типів автентифікації та кілька технологій, які можна використовувати для автентифікації між незалежними рішеннями із загальним та централізованим джерелом повноважень. Федерація ідентичності існує у багатьох формах, але мета та функції майже однакові. Використовуйте центральний каталог, щоб підтримувати ідентифікатори та паролі користувачів, які можуть надавати доступ до незалежного рішення без необхідності мати кілька сховищ користувачів.

Найпоширенішою метою Федерації ідентифікаційних даних є надання або скасування доступу користувача з одного місця до декількох служб. Таким чином, користувач може прийти і піти з вашої організації. Вам не потрібно керувати обліковими записами користувачів та авторизацією у кожній окремій системі, що є у вашому підприємстві[11-13]. Поняття Федерації ідентичності є загальним, і існує кілька основних технологій, які можна використовувати для отримання цього дозволу з одного центрального місця.

Тепер те, що дозволяє Федерація ідентичності, - це єдиний вхід, який також називають SSO. Це означає, що управління користувачами та автентифікація користувачів відбуватимуться з одного сховища ідентифікаторів, і ідентифікація визначатиме рівень доступу, який матиме користувач. Отож із системою єдиного входу ви можете використовувати стандартні інструменти для створення та управління ідентифікаторами користувачів.

Приклади включають:AWS Simple AD, Microsoft Active Directory та LDAP, кілька найпоширеніших каталогів, а зверху цих каталогів є інструменти та програми, які можуть створювати SAML, мову розмітки тверджень безпеки, щоб розширити Active Directory до Інтернету, фактично забезпечити шар між сервером AD та Інтернетом. Рівень забезпечує SAML 2.0, відкритий стандарт для автентифікації між службами, і може забезпечити посередника між кількома службами в одному загальному джерелі автентифікації.

Федерація ідентичності AWS підключає зовнішніх користувачів до AWS через роль IAM, яка налаштована на надання доступу. З цієї ролі користувач може отримати доступ до дозволеного цією роллю в AWS. Зовнішній постачальник ідентифікаційних даних автентифікує користувача. Ролі IAM облікового запису AWS дозволяють користувачеві виконувати операції над ресурсами облікового запису AWS. Існує дві різні фази, автентифікація з джерелом SSO та авторизація, що надаються Роллю управління доступом до ідентичності AWS, призначеною цьому користувачеві.

2.5. Управління обліковими записами та доступом

Хмарні провайдери можуть підтримувати деталізацію в IAM, яка перевищує норму традиційної інфраструктури. Це уможливлює нові моделі безпеки, такі як контроль доступу на основі атрибутів.

Визначимо, які ролі можуть бути в хмарній інфраструктурі, як це зображено на рисунку 2.4. На нижньому ярусі у нас завжди буде наш мастер акаунт, який буде мати найвищий рівень доступу і може робити все в хмарі. Очевидно, що цей акаунт повинен бути найзахищенішим. Над ним буде акаунт менеджера- супер адміна, який

буде мати всі привілегії рута, окрім того, що він може впливати на акаунт мастер. Це важливо, оскільки, якщо хтось дискредитує акаунт супер адміна, тоді зможемо зайти під акаунтом мастера та забрати права в супер адміна, ось чому акаунт рута настільки важливий.

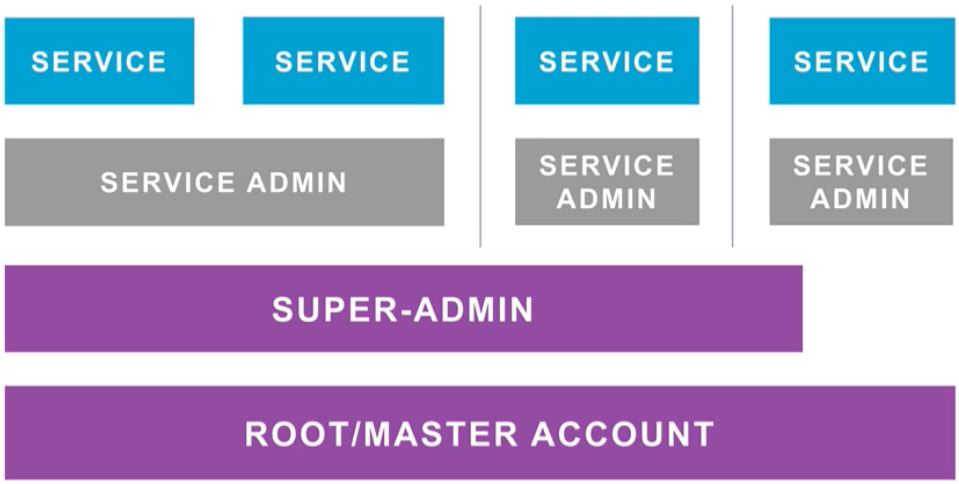

Рис.2.4 – Розподіл ролей в хмарній інфраструктурі

Рекомендації, полягають в тому, щоб створити акаунт мастера, заховати MFA(multifactor authentication) токен в сейф та більше не користуватися ним, лише у разі крайніх ситуацій, як було наведено вище.

Звісно, якщо не хочемо, щоб всі в нашій інфраструктурі були суперадміністраторами, тому маємо концепцію адміністраторів ссервісів. Наприклад, адміністратор для менеджменту віртуальних машин та віртуальної мережі може бути однією людиною, також можемо мати одного адміністратора для певного окремого сервісу.

В хмарній інфраструктурі відходимо від конторолю доступу, що базується на ролях (RBAC) до контролю доступу за атрибутами (ABAC). Контроль доступу на основі ролей (RBAC) та контроль доступу на основі атрибутів (ABAC) - це два способи контролю процесу аутентифікації та авторизації користувачів. Основною відмінністю між RBAC та ABAC є те, що RBAC забезпечує доступ до ресурсів або інформації на основі ролей користувачів, тоді як ABAC надає права доступу на

основі атрибутів користувача, середовища чи ресурсу. По суті, розглядаючи RBAC проти ABAC, RBAC контролює широкий доступ в межах організації, тоді як ABAC застосовує тонкозернистий підхід.

SaaS та хмарні додатки створили більш складну реальність на фронті безпеки - реальність, в якій, наприклад, додатки, як правило, розміщуються на сторонній інфраструктурі та запускають сторонній код. У цьому новому, динамічному та менш контрольованому середовищі дозволи є значно складнішими, і RBAC не завжди може задовольнити потреби безпеки.

Особливість SaaS "розгортання в будь-який час і в будь-якому місці" - це не тільки підвищена зручність, але й реальний і зовсім інший вид ризику.

Здається, все більша кількість підприємств переймає, усвідомлюючи, що вони повинні різко змінити підхід до авторизації та безпеки даних. В іншому поколінні авторизація часто давалася на основі заздалегідь визначених привілеїв - але це вже минуле. Зовсім інша стратегія полягає у визначенні привілеїв доступу на основі тут і зараз, це єдиний природний шлях вперед.

ABAC має більш ширший підхід, це технологія, яка забезпечує більш комплексне рішення авторизації та проблем безпеки[13-15]. Контроль доступу на основі атрибутів базується на наборі характеристик, які називаються "атрибутами". Сюди входять атрибути користувача, атрибути середовища та атрибути ресурсу.

Атрибути користувача включають такі речі, як ім’я користувача, роль, організація, ідентифікатор та дозвіл на безпеку.

Атрибути навколишнього середовища включають час доступу, розташування даних та поточний рівень організаційної загрози.

Атрибути ресурсу включають такі речі, як дата створення, власник ресурсу, ім'я файлу та чутливість даних.

По суті, ABAC має набагато більшу кількість можливих змінних управління, ніж RBAC. ABAC впроваджено для зменшення ризиків через несанкціонований доступ, оскільки він може контролювати безпеку та доступ на більш детальній основі. Наприклад, замість того, щоб люди, які виконують роль HR, завжди могли отримати доступ до інформації про співробітників та заробітну плату, ABAC може

встановити додаткові обмеження щодо їх доступу, наприклад, дозволяти це лише протягом певного часу або для певних філій, що стосуються відповідного працівника. Це може зменшити проблеми із безпекою, а також може допомогти у подальшому процесі аудиту, Полегшуючи авторизацію в середовищах, що динамічно змінюються, це сприяє швидшому впровадженню нових інструментів і, що найважливіше, може допомогти компаніям уникнути мінливого доступу.

Ось чому Gartner вже передбачав, що до 2020 року вражаючі 70% усіх підприємств будуть використовувати ABAC. Порівняйте з 5% підприємств, які використовували його в не такому й далекому 2017, це вражаюче передбачення. ABAC забезпечує більш практичний стандарт, який забезпечує швидші та безпечніші способи додавання та видалення доступу до програм та служб.

Це добре підходить для нашої нової реальності - реальності ділового середовища без будь-якого фізичного периметру. Платформи, що використовують надійні стандарти авторизації, будуються та розробляються з урахуванням цього головного зрушення та з урахуванням того, що сьогодні підприємствам потрібно продовжувати підтримувати безпеку, підтримувати постійно мінливий пул SaaS та хмарних додатків та налаштовувати зовнішні групи користувачів як партнери, замовники та працівники за контрактом. І в час загострення проблем із безпекою підхід, який надає ABAC, необхідний для захисту, управління та спільного використання активів даних.

Зростаюча тенденція SaaS та хмарних платформ ще більше ускладнює необхідність посилення контролю за управлінням ідентифікацією. При правильному застосуванні стандартів доступу та протоколів підприємства можуть гарантувати, що вони знають, хто і коли отримує доступ до ресурсів компанії з усіх куточків інфраструктури.

2.6. Реагування на інциденти

Сьогодні витрати на простої для підприємств, що залежать від центрів обробки даних, ростуть швидше, ніж в середньому. А коли час простою обходиться

в середньому майже в 9000 доларів за хвилину, підприємствам необхідно знайти способи зниження ризиків та управління інцидентами швидко і ефективно.

Управління реагуванням на інциденти - непомічений герой розробки програмного забезпечення та IT-операцій. Хороший процес реагування на інциденти працює за лаштунками, щоб гарантувати швидке рішення проблем, щоб зв'язок, продуктивність і розробка могли продовжувати працювати безперешкодно[16-18].

Інцидент - це незапланованe переривання або зниження якості IT-послуги. У світі, де надійність має вирішальне значення для запобігання дорогому простою та пом'якшення ризиків безпеки та бізнесу, компанії повинні інвестувати в надійний процес управління реакцією на інциденти. Традиційне управління IT-послугами (ITSM) покладається на безліч програм і платформ для моніторингу, відстеження та попередження команд про інциденти в процесі їх розвитку.

Оскільки інциденти впливають на продуктивність, простою та навіть безпеку, IT-командам важливо швидко та точно реагувати (і навіть передбачати) проблеми. Однак традиційні ITSM просто не можуть встигнути за швидкістю сучасних команд розробників. DevOps покладається на прозорість, співпрацю та швидкість для швидкого розгортання. Реагування на хмарні події робить це можливим. Хмарне реагування на аварії об’єднує всі ці функції в одне місце для спрощеної та ефективної системи реагування на аварії, що включає моніторинг, зв’язок, документацію та оповіщення. Як результат, команди реагування на хмарні інциденти краще підготовлені для співпраці, відстеження процесів та автоматизації ключових завдань безпеки.

Було розроблено декілька правил, яким варто слідувати, задля забезпечення вчасного реагування на інциденти. По-перше, варто нагадати, що зберігання та транслювання великої кількості даних в хмарі має свою ціну. Тому, порада полягає в тому, щоб максимально використовувати власне сховище, щоб зменшити вартість за зберігання, а також не надсилайте все по мережі. На рисунку показана схема архітектури множинних облікових записів. У нас є три глобальних модуля: розробники, тестери та продакшн. Вони всі можуть зберігати свої логи в спільному лог акаунті і все це в рамках цього одного проекту. Переваги даної архітектури

полягають в тому, що ваш адміністратор проекту буде бачити всі логи та зможе використовувати їх для звичайного усунення неполадок. Також, вони будуть скопійовані і передані до центру безпеки, куди вже адміністратор проекту не матиме доступу, а для ще детальнішого розслідування компанія захоче передати логи до певного аналітичного сервісу, для прикладу QRadar, який може бути розвернутий як в хмарі, так і в фізичній інфраструктурі, як це зображено на рисунку 2.5. Ключові аспекти включають:

1. Фільтрування логів перед тим як передавати їх через інтернет. Оскільки всі хмарні провайдери стягують плату за передані байти.

2. Логи з проектів повинні бути доступні для читання для адміністраторів проекту через базу даних проекту.

3. Потрібно корелювати, звідки прийшли логи перед тим як їх відпраляти, оскільки в разі порушення, потрібно точно знати де саме в хмарі сталася несправність.

4. Розробити посібники зі стандартними процедурами реагування на інциденти. Процес управління реакцією на події допомагає вам:

a. Швидше вирішити інциденти

b. Поліпшити внутрішнє та зовнішнє спілкування

c. Зменшити втрати доходу

d. Сприяти постійному навчанню та вдосконаленню

e. Описати сценарії, яким ваша команда може слідувати, щоб спілкуватися із замовниками та зацікавленими сторонами щодо критичних відключень. Переконайтесь, що ваші процеси регулярно оновлюються (автоматизуйте, де це можливо), і щоб члени команди мали доступ до навчальних посібників.

f. Складання плану відновлення гарантує, що ви готові швидко та впевнено вирішувати випадки, зменшуючи ризик дорогих помилок та плутанини.

g. Визначте свої пріоритети та ступінь тяжкості до того, як трапиться інцидент, щоб менеджери інцидентів могли швидко оцінити та визначити пріоритети у розпал моменту. Розглядайте всі майбутні інциденти в порядку пріоритетності.

5. Записуйте і класифікуйте кожен інцидент. Кожен інцидент, як правило, повинен містити:

a. Ім'я особи, яка повідомляє про інцидент
b. Дата та час звіту
c. Опис інциденту (що не працює)
d. Унікальний ідентифікатор для відстеження цього інциденту[18-24].

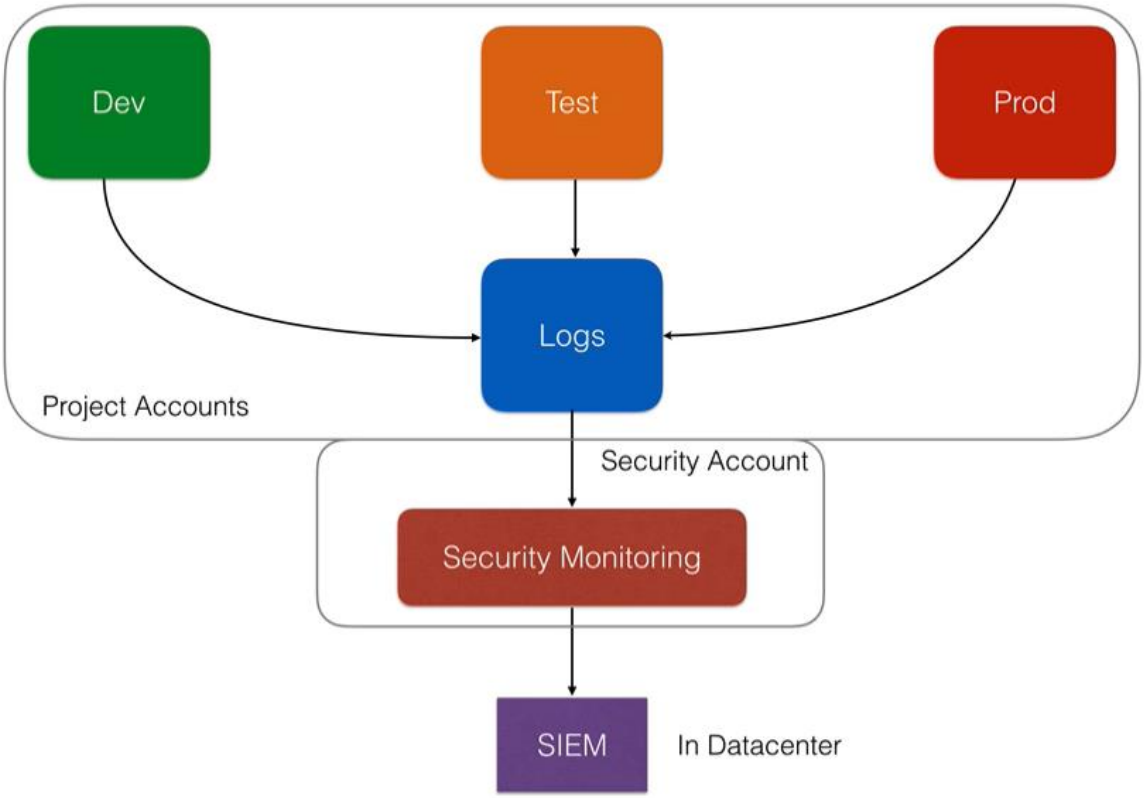

Рис.2.5 – Схема архітектури для безпечного реагування на інцинденти

Висновки за розділом 2

У даному розділі було проведено ряд досліджень та отримано наступні практичні результати:

По-перше, проаналізовано передумови для висування вимог до хмарних систем, що створює контекст для вибору технологічного рішення.

По-друге, проведено дослідження як побудована програмно-конфігурована мережа.

По-третє, доведено необхідність використання комплексного підходу для сегрегації мережі.

По-четверте, розглянуто архітектуру запропонованої технології.

По-п’яте, наведено аргументування відносно того, як групи безпеки забезпечують відповідний рівень захисту, який в фізичній інфраструктурі забезпечують брандмауери.

По-шосте, наведено пояснення як забезпечується ідентифікація доступу в хмарі за допомогою третьої сторони. Наведено приклад працюючої політики з управління обліковими записами та доступом та запропоновано архітектуру множинних облікових записів та найкращі практики для вчасного реагування на інциденти.

РОЗДІЛ 3
ТЕХНІЧНА РЕАЛІЗАЦІЯ КОМПЛЕКСНОГО РІШЕННЯ ДЛЯ ЗАХИСТУ ХМАРНОЇ АРХІТЕКТУРИ

1.1. Налаштування віртуальної приватної хмари (VPC)

Для практичної частини диплому буде використовуватися Amazon Web Services network. Для початку потрібно визначити тип віртуальної мережі, для цього перейдемо до vpc, що розшифровується як віртуальна приватна хмара. На додаток до загальнодоступної підмережі, для повноти роботи, вибрана мною конфігурація додає приватну підмережу, екземпляри якої неможливо адресувати з Інтернету. Екземпляри в приватній підмережі можуть встановлювати вихідні підключення до Інтернету через загальнодоступну підмережу за допомогою перекладу мережевих адрес

Публічні підмережі екземплярів користувача Elsastic IPs для доступу до Інтернету. Екземпляри приватних підмереж отримують доступ до Інтернету через NAT.

Архітектура мережі зображена на рисунку 3.1.

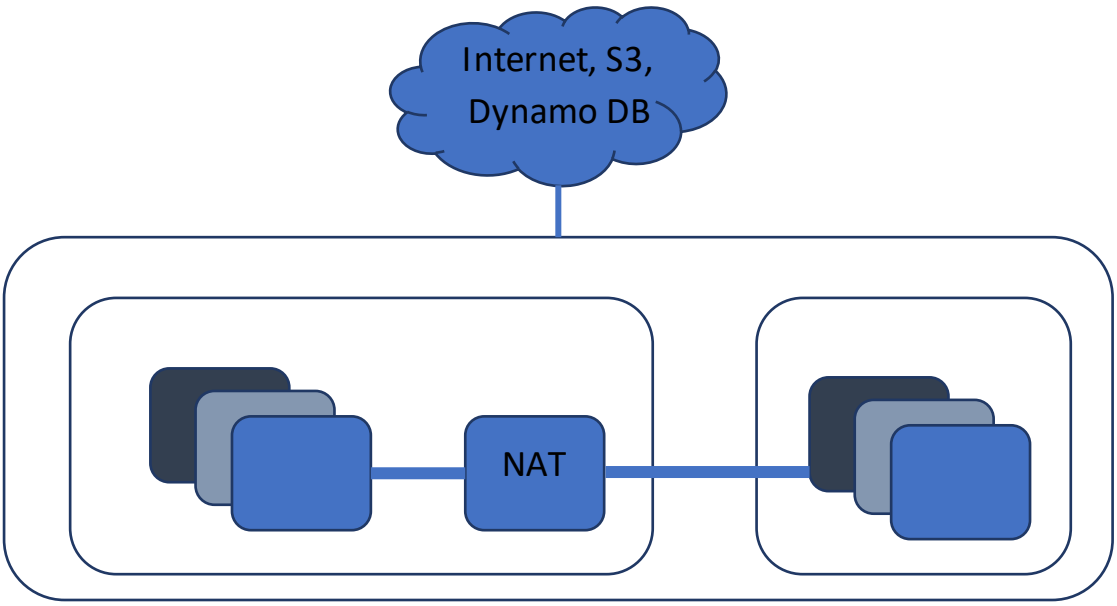

Рис.3.1. Архітектура хмарного сховища

Налаштування будуть виглядати наступним чином, як це зображено на рисунку 3.2.

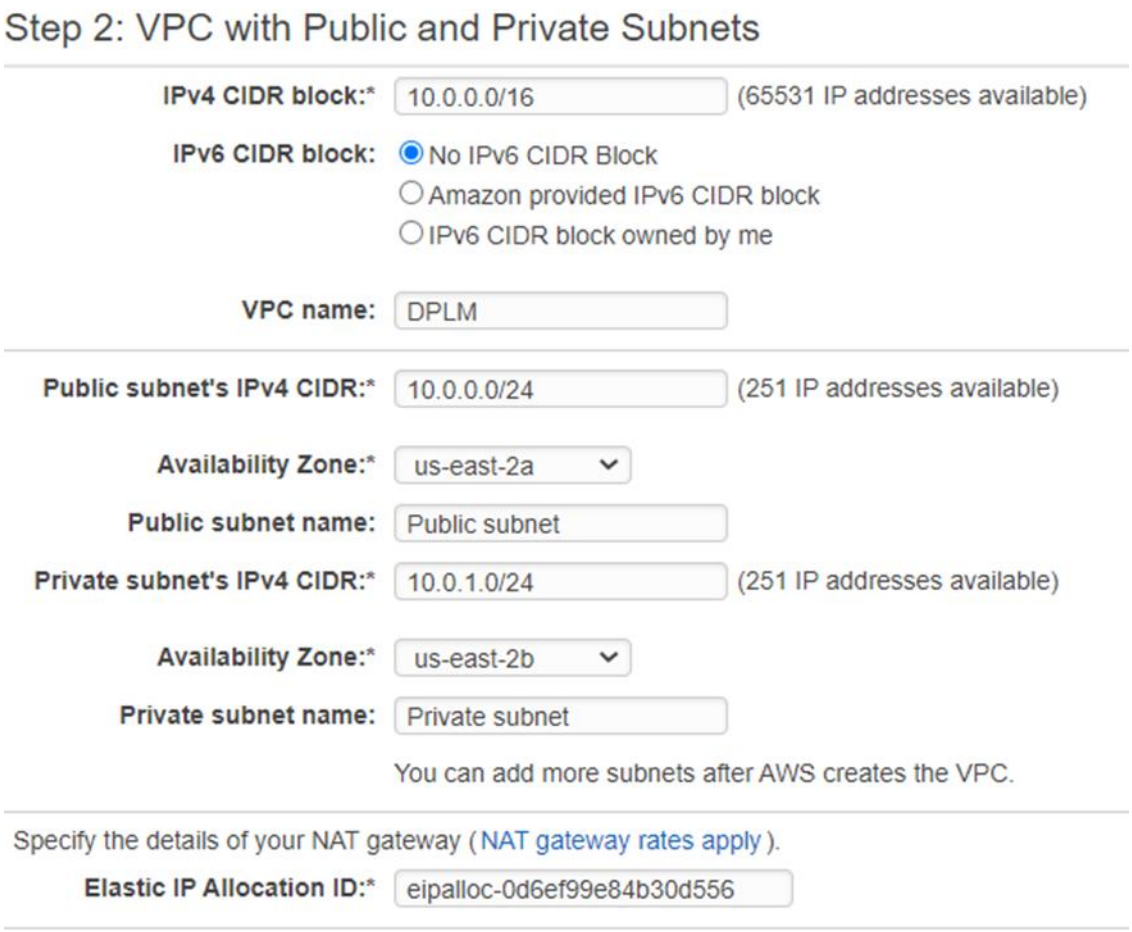

Рис.3.2 – Налаштування конфігурації VPC

Будемо підтримувати лише ipv4. Було вказано ім’я для VPC- DPLM. Оскільки у нас буде дві підмережі, одна з виходом в інтернет, а друга- ні. Публічну підмережу було призначено для певної зони доступності (us-east-2a), зони - це фізично окремі центри обробки даних у межах одного регіону. Тепер для приватної підмережі підберемо наш діапазон адрес, було зіставлено його із зоною доступності us-east-2b, це забезпечить різний набір апаратних засобів, що в свою чергу забезпечить високу стійкість. Це рахується хорошою практикою, розміщувати кілька публічних та приватних підмереж у різних зонах доступності, щоб мати змогу налаштовувати баланс між ними та підтримувати високу доступність.

Наступне, що потрібно налаштувати- це NAT шлюз, що означає транслятор мережевих адрес. Він забезпечує доступ до Інтернету з приватної мережі, але Інтернет не може отримати доступ до приватної мережі. Для цього вам потрібно вказати еластичну ip-адресу, яку ви орендуєте в Amazon.

Наступне, що встановимо, - це кінцеві точки обслуговування. Кінцеві точки обслуговування дозволяють направляти трафік безпосередньо з наших підмереж до інших служб Amazon, коли робимо з'єднання API. Наприклад, якщо потрібно використовувати Amazon DynamoDB або в нашому випадку Amazon S3. Зазвичай екземпляр повинен здійснити виклик API на s3.amazonaws.com, тобто це означає, що у приватній мережі ви повинні мати інтернет, але що, якщо потрібно мати приватну підмережу без виходу в інтернет, і все ще потрібно дозволити їй мати доступ до S3. Тоді потрібно лише налаштувати там кінцеву точку, і ось що кінцеві точки забезпечують, вони буквально фіксують dns запит і направляють його внутрішньо. Було підключено його як до загальнодоступних, так і до приватних підмереж. Зроблено це для економії коштів, оскільки тоді трафік не буде виходити за межі мережі, і можна заощадити трохи грошей, отримавши внутрішній доступ до s3, як це зображено на рисунку 3.3.

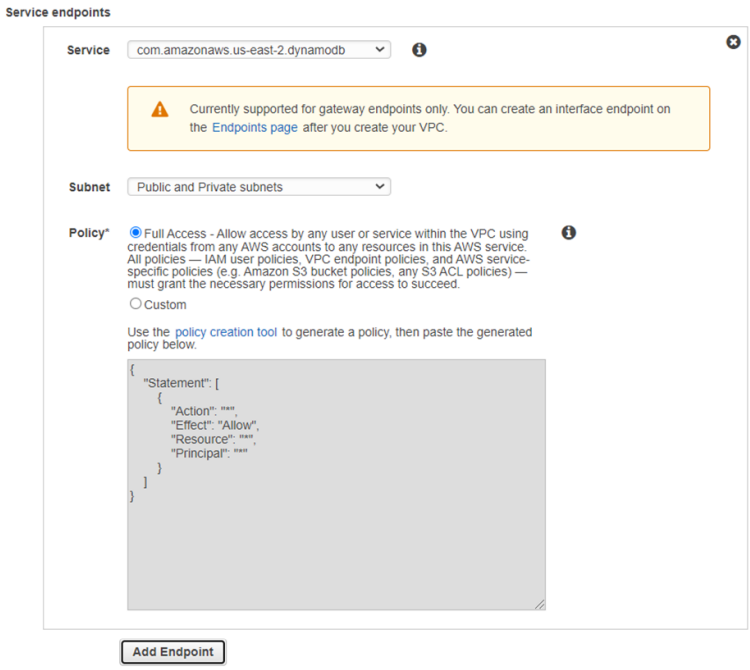

Рис.3.3 – Налаштування service endpoint

Після того як VPC створився, можемо побачити інформацію про нього, яка включає в себе деталі, CIDRs де знаходиться інформація про IP адреси, Flow logs, які ви можете перенаправляти в ваш SIEM (Qradar), як це зображено на рисунку 3.4.

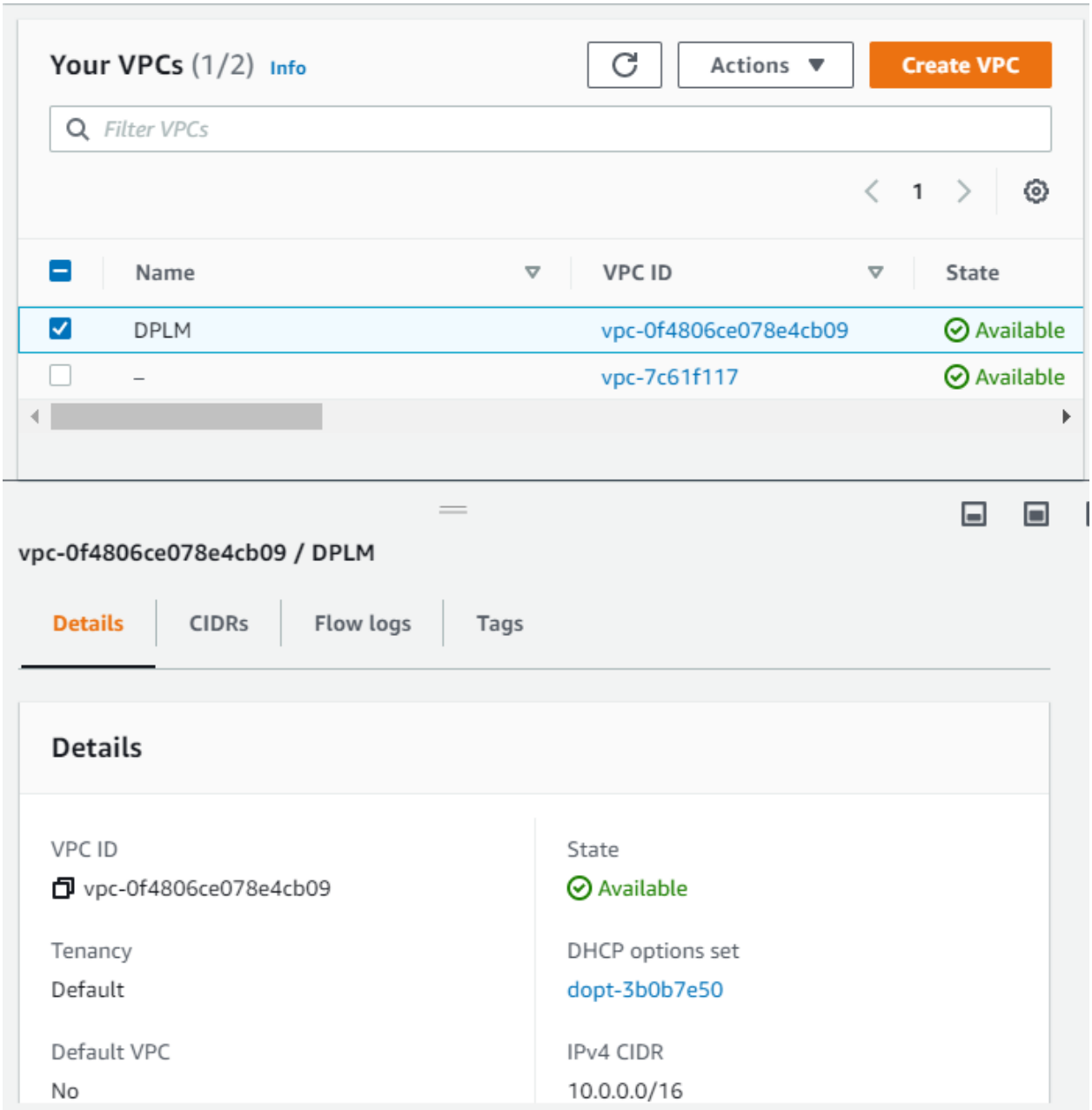

Рис.3.4 – Перевірка коректного налаштування VPC

Якщо перейдемо в розділ route tables можемо побачити, що дані з публічної підмережі транслюються через igw (internet getaway), а з приватної через nat, як це зображено на рисунку 3.5.

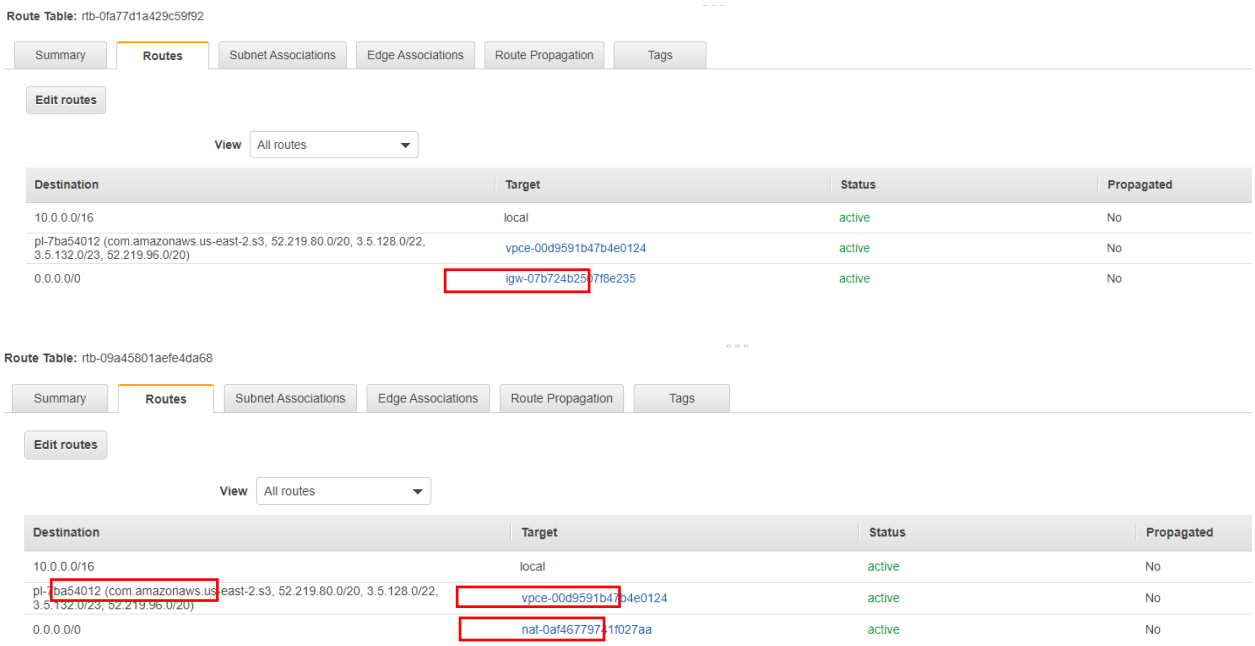

Рис.3.5 – Перевірка коректного налаштування інтернет шлюзу та NAT

Також тут видно, що коли збираємося зв'язатися з s3, то наш трафік проходить через vpce (virtual private cloud endpoint).

Наступний важливий крок – формування груп безпеки.

Після цього переходимо в групи безпеки, де створюємо групу для вебсайтів, в якій прописуємо правило, що буде дозволено лише захищений трафік з інтернету, тобто в source прописуємо ip адресу 0.0.0.0/0 та обираємо протокол HTTPS, порт 443. Групи безпеки не під'єднані до підмереж, ви можете визначити їх до інтсансів чи покажчика нагрузки, потрібно дивитися на групи як на об'єкти, що взаємодіють з об'єктами, як це зображено на рисунку 3.6.

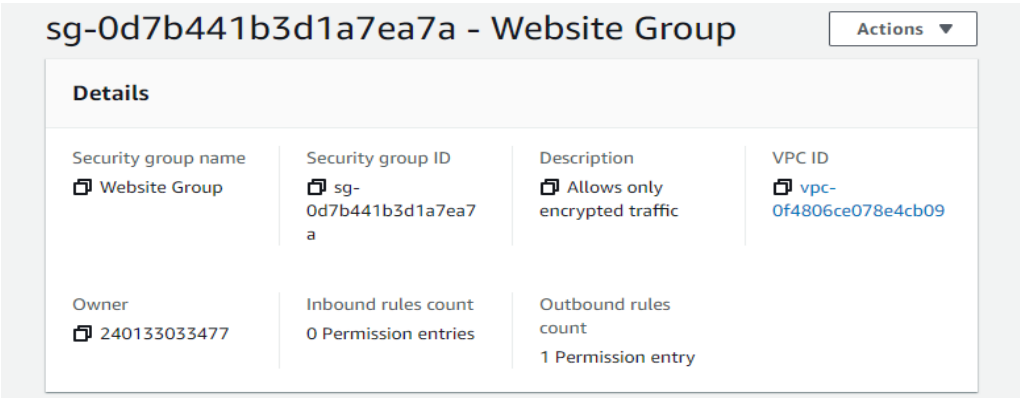

Рис.3.6 – Створення групи безпеки

Також групи безпеки не залежать від зон доступності. Для прикладу було створено ще одну групу, яка отримує трафік від іншої групи, та визначено порт 3306, що відповідає за sql, це означає що ця група буде приймати трафік бази даних від іншої групи безпеки, наприклад від потрібного додатка, як це зображено на рисунку 3.7.

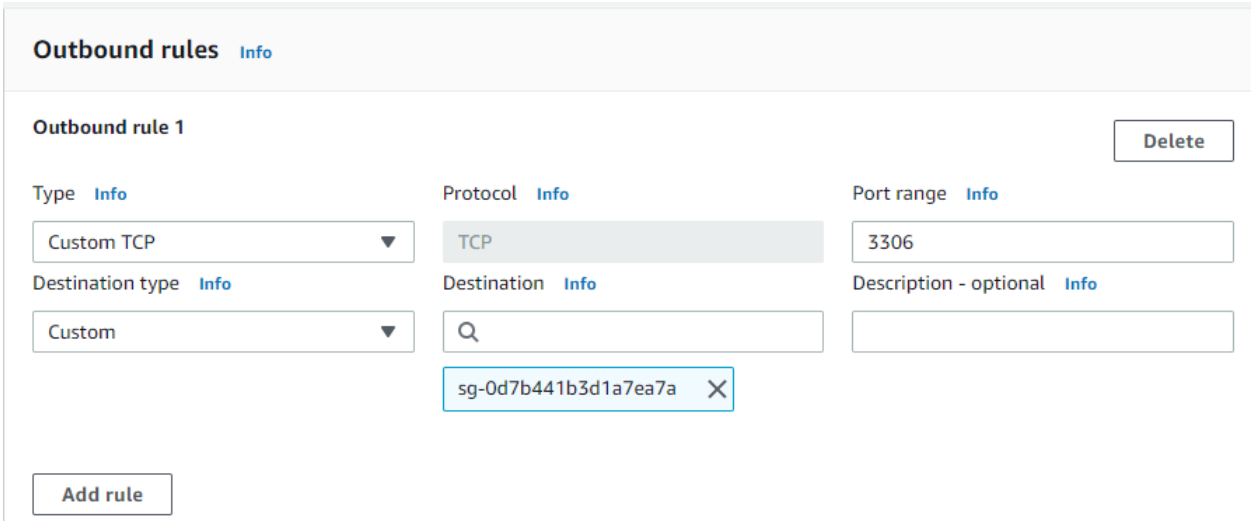

Рис.3.7 – Налаштування відповідних правил до групи безпеки

Якщо ви запускаєте екземпляр за допомогою API Amazon EC2 або інструмента командного рядка, і ви не вказуєте групу безпеки, екземпляр автоматично призначається групі безпеки за замовчуванням для VPC[24]. Якщо ви запускаєте екземпляр за допомогою консолі Amazon EC2, у вас є можливість створити нову групу безпеки для екземпляра.

1.2. Налаштування IAM

Налаштування ідентифікації контролю доступу в AWS слід розпочати з розуміння примітивів, тобто на чому побудовані IAM в хмарних провайдерів.

Ви керуєте доступом в AWS, створюючи політики та приєднуючи їх до ідентифікаторів IAM (користувачів, груп користувачів або ролей) або ресурсів AWS. Політика - це об’єкт в AWS, який, пов’язаний із ідентифікатором або ресурсом, визначає їхні дозволи. AWS оцінює ці політики, коли довідник IAM (користувач або

роль) робить запит. Дозволи в політиках визначають, дозволено чи відхилено запит. Більшість політик зберігаються в AWS як документи JSON.

Політики, що базуються на ідентичності, - це документи політики дозволів JSON, які контролюють, які дії може виконувати особа (користувачі, групи користувачів та ролі), на яких ресурсах та за яких умов. Політику, що базується на особистості, можна додатково класифікувати:

1. Керовані політики - автономні політики на основі ідентифікаційних даних, які можна приєднати до кількох користувачів, груп та ролей у своєму обліковому записі AWS. Існує два типи керованих політик:

a. Керовані політики AWS - керовані політики, які створюються та керуються AWS.

b. Політики, керовані клієнтами - Керовані політики, які ви створюєте та керуєте у своєму обліковому записі AWS. Політики, керовані клієнтами, забезпечують точніший контроль над вашими політиками, ніж політики AWS.

2. Вбудовані політики - політики, які ви додаєте безпосередньо до одного користувача, групи чи ролі. Вбудовані політики підтримують суворі взаємні взаємозв'язки між політикою та ідентичністю. Вони видаляються, коли ви видаляєте особу[26-27].

Наступне- це ролі. Роль IAM - це ідентифікатор IAM, який ви можете створити у своєму обліковому записі з певними дозволами. Роль IAM схожа на користувача IAM, оскільки вона є ідентифікацією AWS із політиками дозволів, яка визначає, що ідентичність може і що не може робити в AWS. Однак замість того, щоб бути однозначно пов’язаною з однією людиною, роль призначена для того, щоб її міг виконувати кожен, хто її потребує. Крім того, роль не має стандартних довгострокових облікових даних, таких як пароль або ключі доступу, пов'язані з нею. Натомість, коли ви берете на себе роль, вона надає вам тимчасові облікові дані безпеки для сеансу ролі.

Ви можете використовувати ролі для делегування доступу користувачам, програмам або службам, які зазвичай не мають доступу до ваших ресурсів AWS. Наприклад, ви можете надати користувачам у вашому обліковому записі AWS

доступ до ресурсів, яких вони зазвичай не мають, або надати користувачам в одному обліковому записі AWS доступ до ресурсів в іншому обліковому записі[28-30]. Або ви можете дозволити мобільному додатку використовувати ресурси AWS, але не хочете вбудовувати ключі AWS у програму (де їх важко обертати та де користувачі можуть потенційно їх витягти). Іноді ви хочете надати AWS доступ користувачам, які вже мають ідентифікаційні дані, визначені поза AWS, наприклад, у вашому корпоративному каталозі. Або, можливо, ви захочете надати доступ до свого облікового запису третім особам, щоб вони могли провести аудит ваших ресурсів.

Для початку, було зроблено кілька речей:

1. Створено нові облікові записи для розробників (та команду розробників). Ви можете керувати ними через організації AWS та обмежувати ресурси, які вони можуть запускати, за допомогою політик організації, як це зображено на рисунку 3.8.

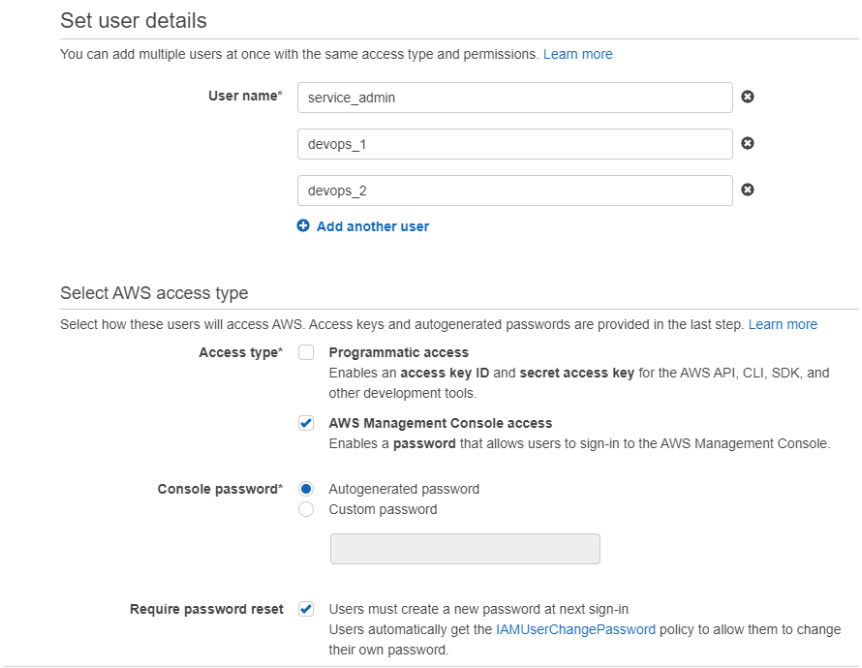

Рис.3.8 – Створення нових ролей

2. Дала розробникам дозволи PowerUser у цих облікових записах - вони зможуть робити все, крім створення інших дозволів IAM та користувачів, як це зображено на рисунку 3.9.

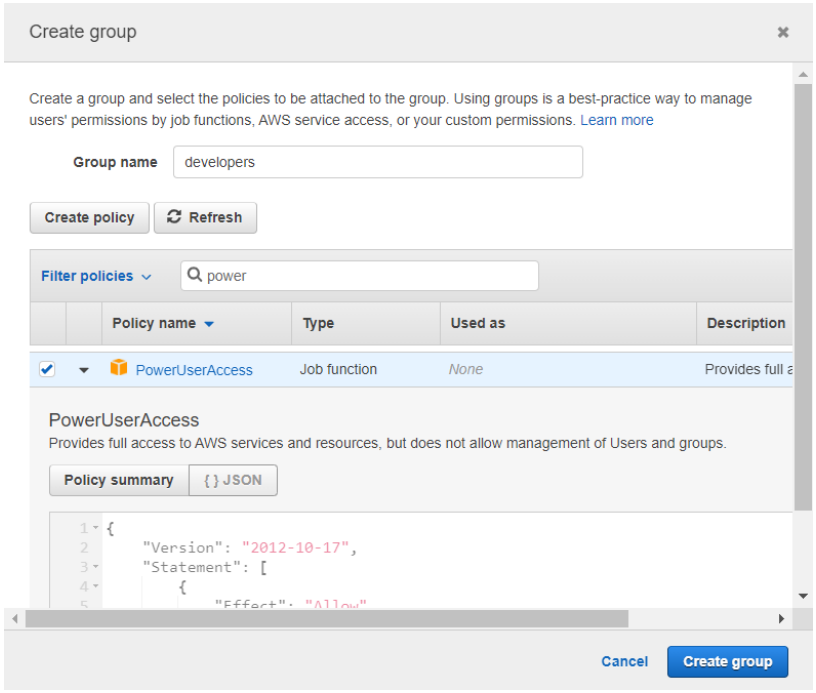

Рис.3.9 – Створення відповідної групи під ролі

Політика наведена на рисунку 3.10.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "account:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:DeleteServiceLinkedRole",
                "iam:ListRoles",
                "organizations:DescribeOrganization",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Рис.3.10 – Політика безпеки до відповідної групи

Також, було створено групу адміністраторів, для яких написано власну політику, яка зображена на рисунку 3.11.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Action":"*",
            "Resource":"*",
            "Condition":{
                "StringEquals": {
                    "ec2:Region":"us-east-2a"
                }
            }
        }
        ]
}
```

Рис.3.11 – Політика безпеки для адміністраторів

Вона буде дозволяти все, в межах певної зони, в нашому випадку це us-east-2a, як це зображено на рисунку 3.12.

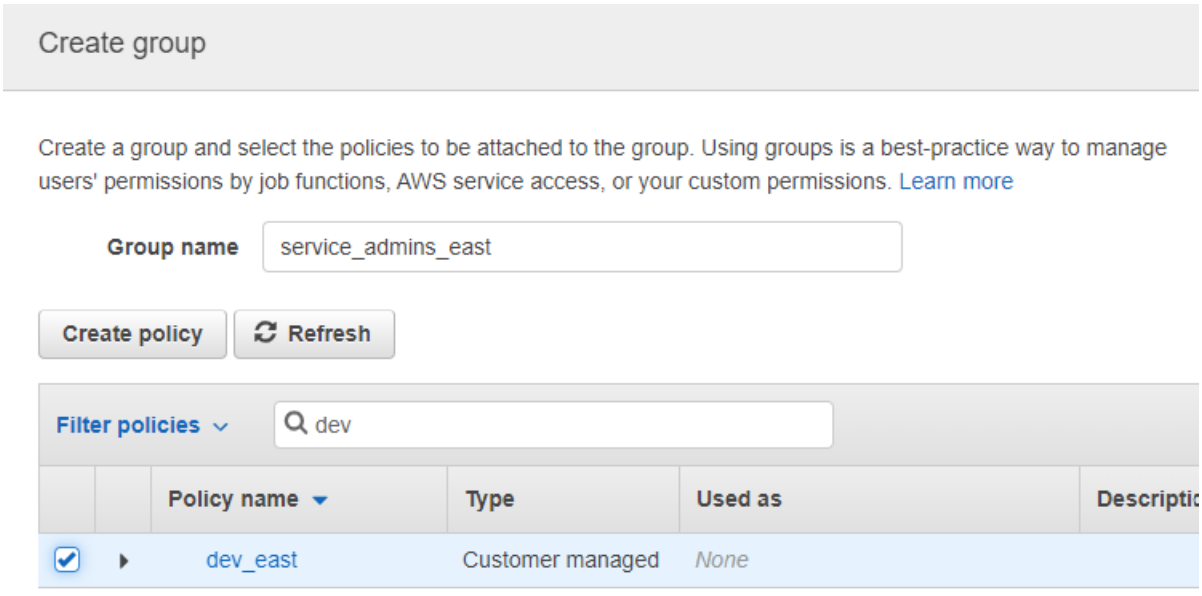

Рис.3.12 – Прив’язка групи до політики безпеки

1.3. Налаштування систем реагування на інциденти

Моніторинг безпеки розширюється в хмарі завдяки додаванню рівня управління та загальним властивостям хмарних середовищ. На противагу вище розглянутим проблемам варто імлементувати такі схеми проектування моніторингу: CloudTrail, CloudWatch, Config.

Розглянемо детальніше можливості кожного з них, перед тим як додавати їх до нашої хмарної архітектури. Для початку, розберемося з можливостями Cloud Trail.

AWS CloudTrail - це послуга, яка забезпечує управління, дотримання вимог, оперативний аудит та аудит ризиків вашого облікового запису AWS. За допомогою CloudTrail ви можете реєструвати, постійно відстежувати та зберігати активність облікового запису, пов’язану з діями у вашій інфраструктурі AWS.

CloudTrail надає історію подій діяльності вашого облікового запису AWS, включаючи дії, вжиті через AWS Management Console, AWS SDK, інструменти командного рядка та інші служби AWS. Ця історія подій спрощує аналіз безпеки, відстеження змін ресурсів та усунення несправностей. Крім того, ви можете використовувати CloudTrail для виявлення незвичної активності у ваших облікових записах AWS[30]. Ці можливості допомагають спростити оперативний аналіз та усунення несправностей.

Для початку, серед сервісів обираємо CloudTrail, одразу попадаємо на головну сторінку, яка показує наші API дзвінки. CloudTrail увімкнено у вашому обліковому записі AWS під час його створення. Коли активність відбувається у вашому обліковому записі AWS, ця активність реєструється у події CloudTrail.

Надається можливість легко переглядати події на консолі CloudTrail, перейшовши до історії подій, як це зображено на рисунку 3.13. Бачимо логи з групи автоматичного масштабування, не дивлячись на те, що AWS робить це без нашої участі, все одно отримуємо логи від цього. Ви можете створити стежку за допомогою консолі CloudTrail, AWS CLI або CloudTrail. Як бачимо, можна мати

декілька трейлів в нашому акаунті, наприклад був створений один трейл за замовчуванням, а другий для певної зони, як це зображено на рисунку 3.14.

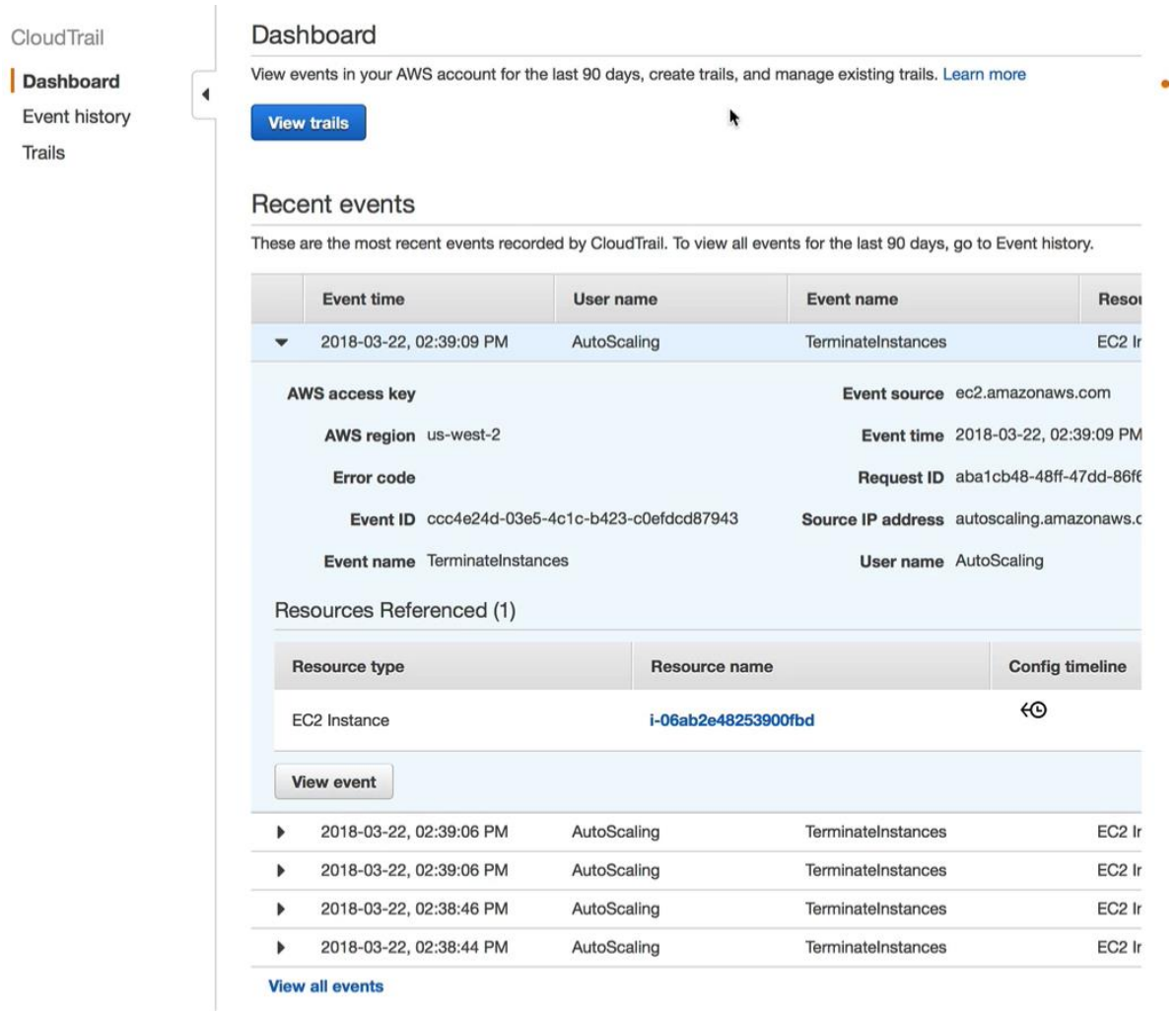

Рис.3.13 – Огляд CloudTrail

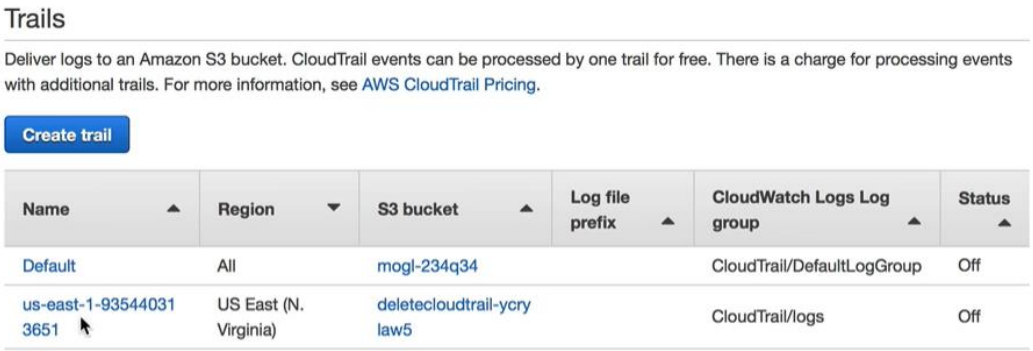

Рис.3.14 – Сортування трейлів за певної зони

Бачимо, що всі логи зберігаються в S3 бакеті, та можемо перенаправляти їх в наш SIEM (QRadar) за допомогою SNS, , як це зображено на рисунку 3.15.

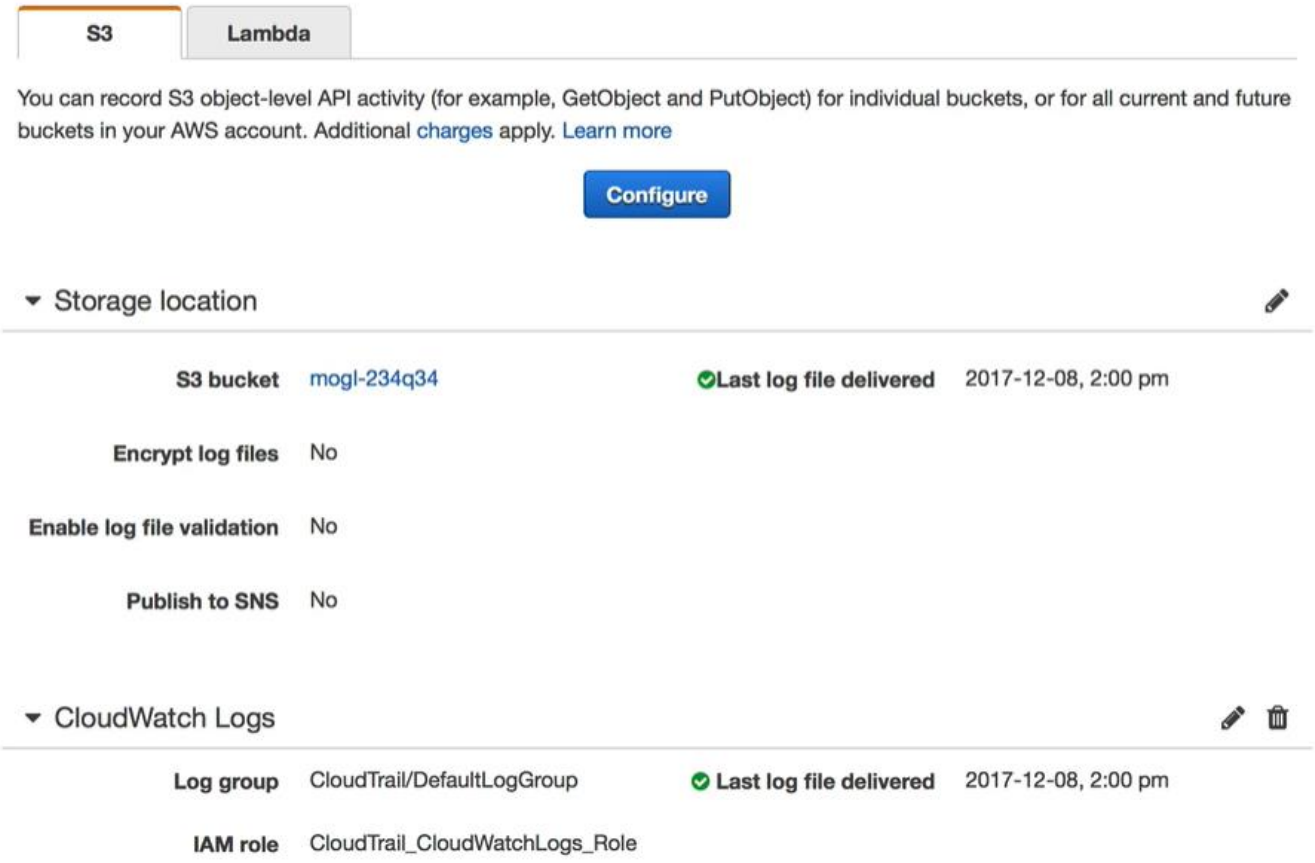

Рис.3.15 – Місце зберігання логів

Якщо перейдемо в цей бакет, то побачимо, що всі логи зберігаються відповідно до зони та сортуються за часовими проміжками, , як це зображено на рисунку 3.16.

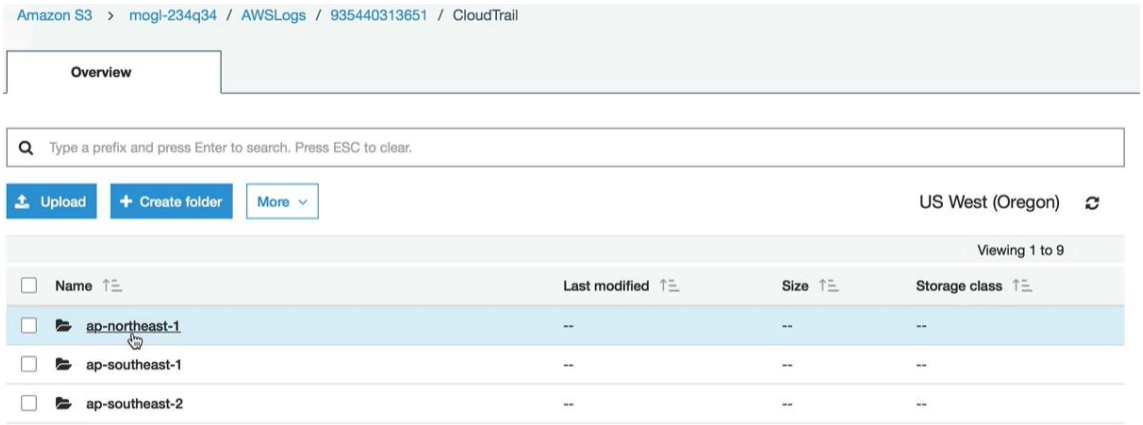

Рис.3.16 – Логи зберігаються відповідно до зони

Можемо переглядати події, вони виглядають наступним чином ти зберігаються в форматі json, , як це зображено на рисунку 3.17.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJNHWVCJA3XUGWMCHC:AutoScaling",
        "arn": "arn:aws:sts::935440313651:assumed-role/AWSServiceRoleForAutoScaling/AutoScalin
        "accountId": "935440313651",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-03-22T21:39:08Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAJNHWVCJA3XUGWMCHC",
                "arn": "arn:aws:iam::935440313651:role/aws-service-role/autoscaling.amazonaws.
                "accountId": "935440313651",
                "userName": "AWSServiceRoleForAutoScaling"
            }
        },
        "invokedBy": "autoscaling.amazonaws.com"
```


Рис.3.17– Приклад лога

В них зберігається інформація, що це за подія, хто взяв на себе роль, що вони зробили, і вся активність, яка з нею асоційована. Історія подій дозволяє переглядати, шукати та завантажувати останні 90 днів активності у вашому обліковому записі AWS. Крім того, ви можете створити маршрут CloudTrail для архівування, аналізу та реагування на зміни у ваших ресурсах AWS. Trail - це конфігурація, яка забезпечує доставку подій до вказаного вами сегмента Amazon S3. Ви також можете доставляти та аналізувати події в результаті за допомогою журналів Amazon CloudWatch та Amazon CloudWatch Events.

Наступний продукт, який будемо імплементувати в нашу архітектуру- CloudWatch. Amazon CloudWatch - це служба моніторингу та управління, яка надає дані та практичну інформацію про AWS, гібридні та локальні програми та ресурси інфраструктури [31-33]. За допомогою CloudWatch ви можете збирати та отримувати доступ до всіх своїх даних про ефективність та експлуатацію у вигляді журналів та показників на одній платформі. Це дозволяє подолати проблему

моніторингу окремих систем та додатків у елеваторах (сервер, мережа, база даних тощо). CloudWatch дозволяє контролювати весь ваш стек (програми, інфраструктура та послуги) та використовувати сигнали тривоги, журнали та події для автоматизованих дій та зменшення середнього часу до роздільної здатності (MTTR), , як це зображено на рисунку 3.18.

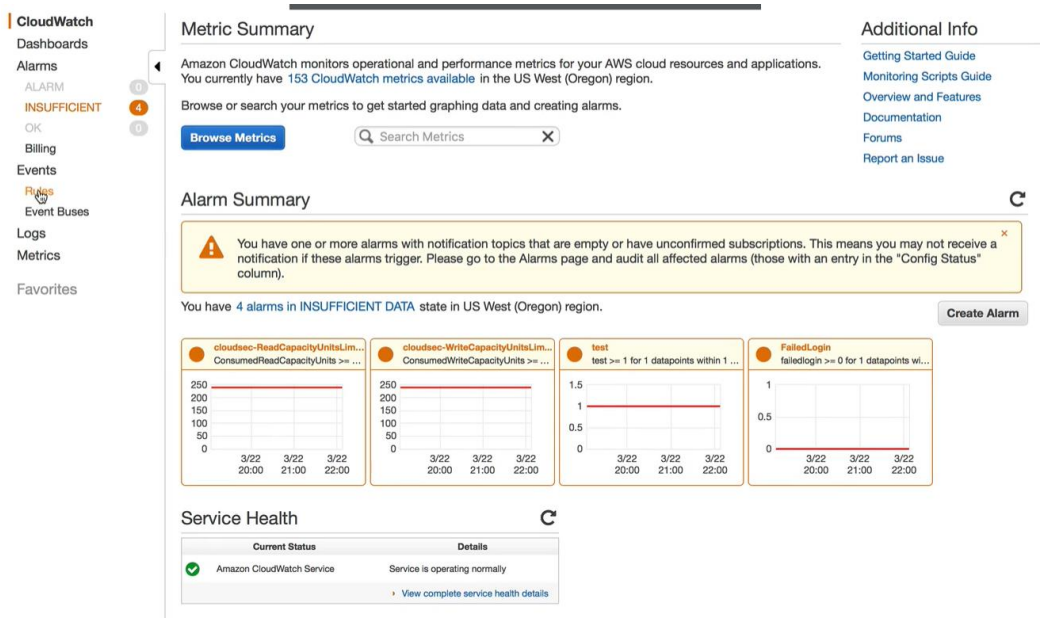

Рис.3.18 – Головна сторінка CloudWatch

CloudWatch надає практичну інформацію, яка допомагає оптимізувати роботу додатків, керувати використанням ресурсів та розуміти загальносистемний стан роботи[34]. CloudWatch забезпечує до 1 секунди видимість метрик та даних журналів, 15 місяців збереження даних (метрик) та можливість виконувати обчислення метрик. Це дозволяє проводити історичний аналіз для оптимізації витрат і отримувати статистику в режимі реального часу щодо оптимізації програм та ресурсів інфраструктури. На основі логів, можемо генерувати правила, , як це зображено на рисунку 3.19.

Наприклад, було згенеровано правило security_group_change, коли в нас api дзвінок до AuthorizeSecurityGroupIngress, щоб створити нове внутрішнє правило безпеки, то одразу спрацьовуватиме тригер, який в моєму випадку є ламбда функція fixSecurityGroup. Це дозволяє мені нативно оснащувати наше середовище та

створювати тригери на основі подій та арі дзвінків, , як це зображено на рисунку 3.20.

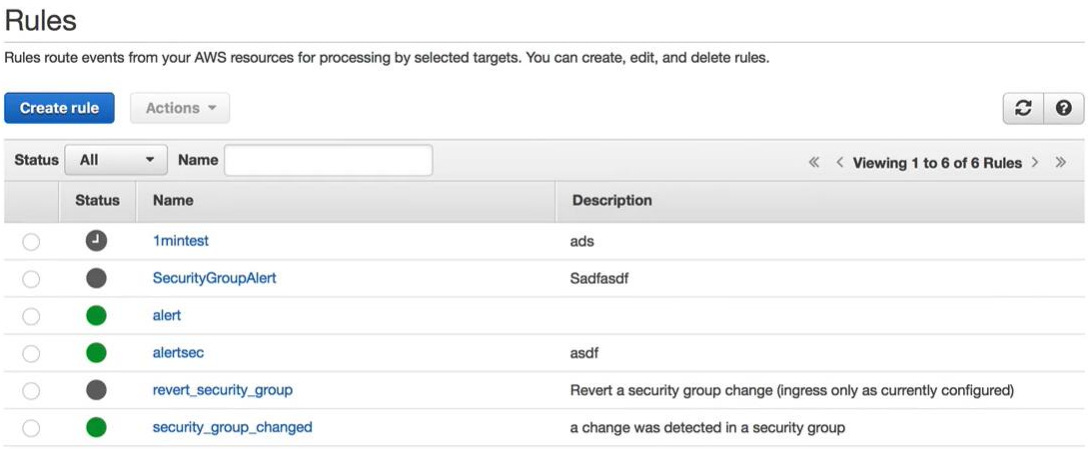

Рис.3.19 – Написання правил в CloudWatch

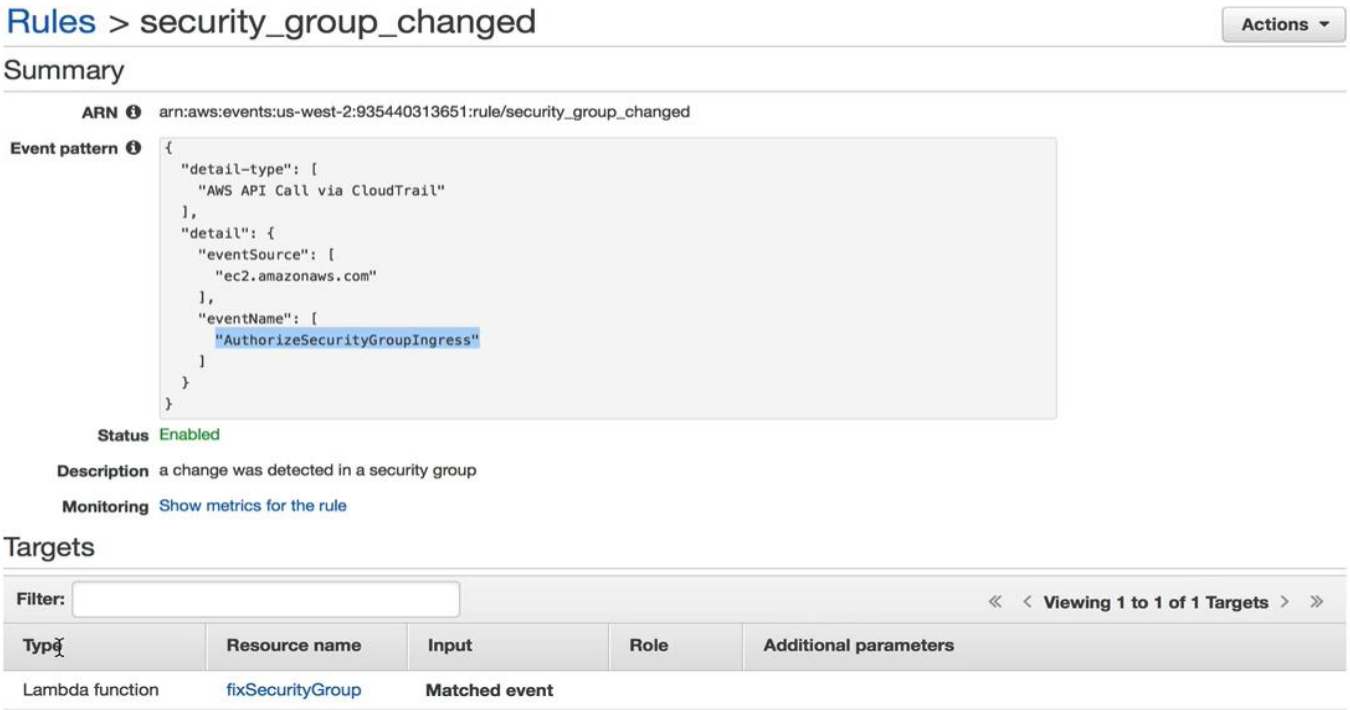

Рис.3.20 – Правило для групи безпеки

Підсумовуючи, Amazon CloudWatch - це в основному сховище метрик. Служба AWS, така як Amazon EC2, розміщує метрики у сховищі, і ви отримуєте

статистику на основі цих метрик. Якщо ви помістили власні показники до сховища, ви також можете отримати статистичні дані щодо цих показників[30].

Третій сервіс, який слід встановити називається AWS Config - це послуга, яка дозволяє оцінювати та перевіряти конфігурації ваших ресурсів AWS. За допомогою Config ви можете переглянути зміни в конфігураціях та взаємозв'язки між ресурсами AWS, заглибитися в детальну історію конфігурації ресурсів та визначити загальну відповідність конфігураціям, зазначеним у внутрішніх правилах. Це дозволяє спростити аудит відповідності, аналіз безпеки, управління змінами та усунення несправностей. Коли ви вмикаєте AWS Config, він спочатку виявляє підтримувані ресурси AWS, які існують у вашому обліковому записі, і генерує елемент конфігурації для кожного ресурсу. За замовчуванням AWS Config створює елементи конфігурації для кожного підтримуваного ресурсу в регіоні, , як це зображено на рисунку 3.21.

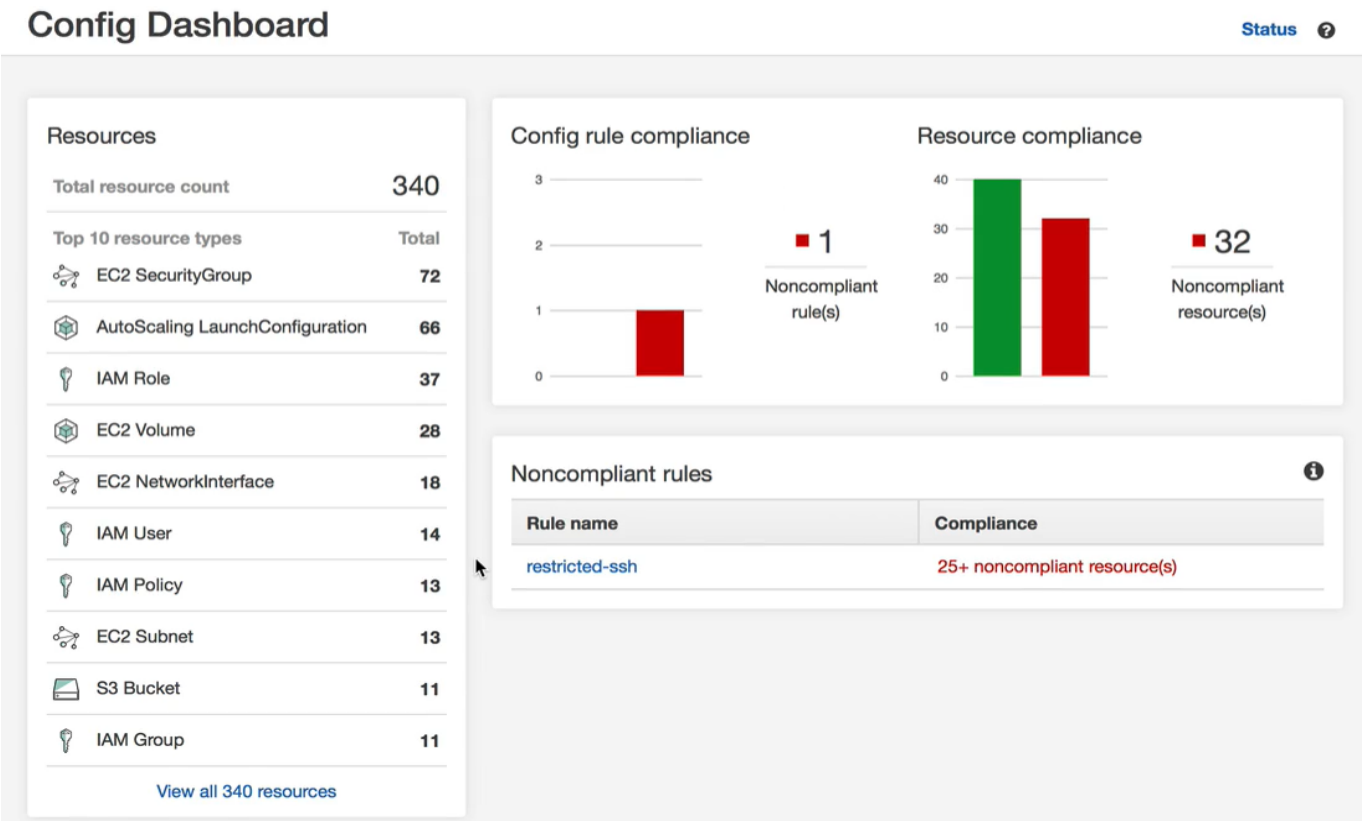

Рис.3.21 – Головне меню Config

AWS Config відстежує всі зміни у ваших ресурсах, викликаючи виклик Describe або List API для кожного ресурсу у вашому обліковому записі. Служба використовує ті самі виклики API для збору деталей конфігурації для всіх пов’язаних ресурсів.

Наприклад, видалення правила виходу з групи безпеки VPC змушує AWS Config викликати API Describe для групи безпеки. Потім AWS Config викликає API Describe у всіх екземплярах, пов’язаних із групою безпеки. Оновлені конфігурації групи безпеки (ресурс) та кожного екземпляра (пов’язані ресурси) записуються як елементи конфігурації та доставляються у потоці конфігурації до сегмента Amazon Simple Storage Service (Amazon S3).

Також він показує наші правила, для прикладу було створено одне, яке було названо restricted_ssh, яке забороняє ssh доступ до усього, та в конфіг можемо переглянути усі групи, які не піддаються цьому правилу, як це зображено на рисунку 3.22.

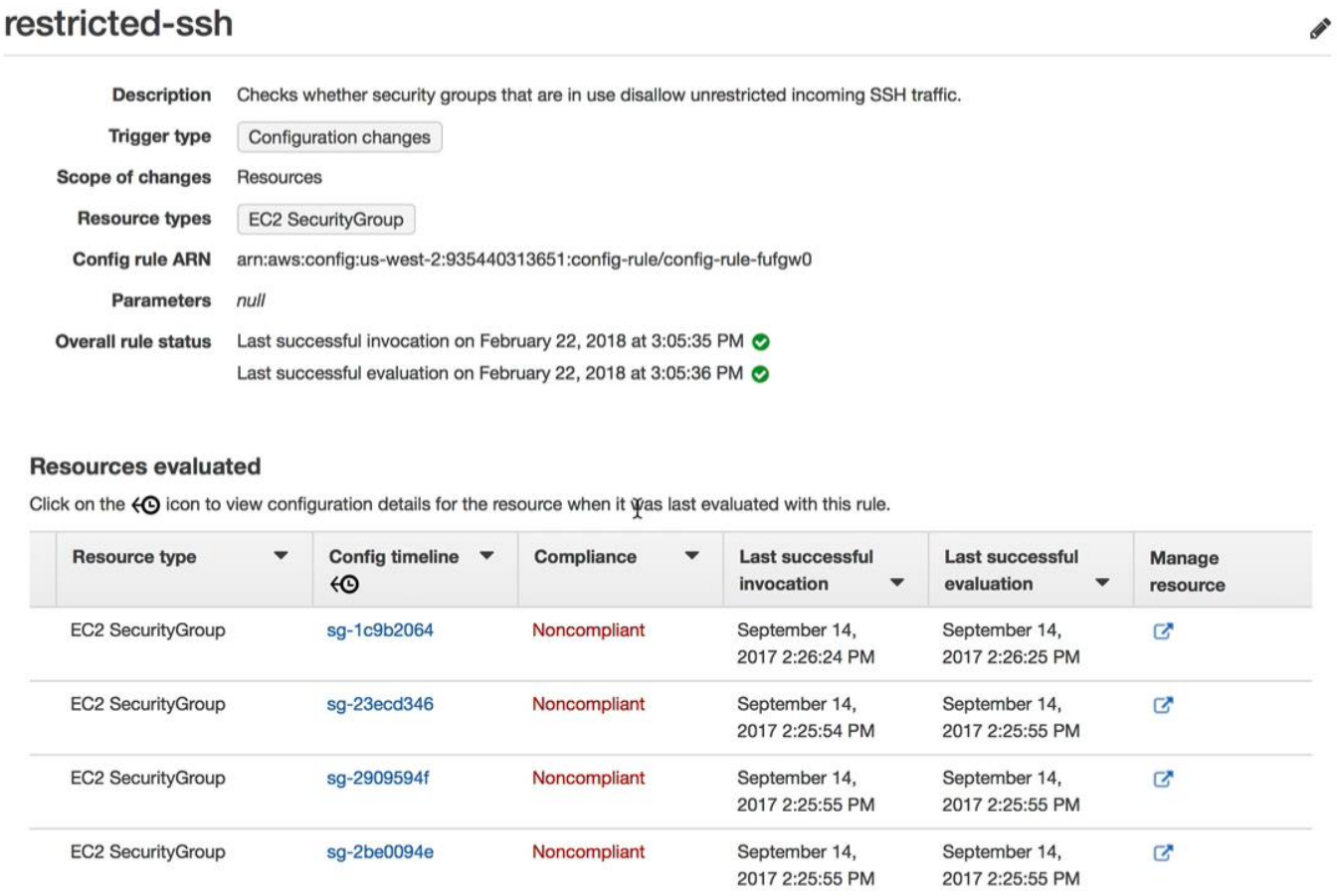

Рис.3.22 – Перегляд груп на які не діє правило

Також в ресурсах можемо обирати всі групи, які нас цікавлять та дивитися з якими правилами вони співставляються, як це зображено на рисунку 3.23.

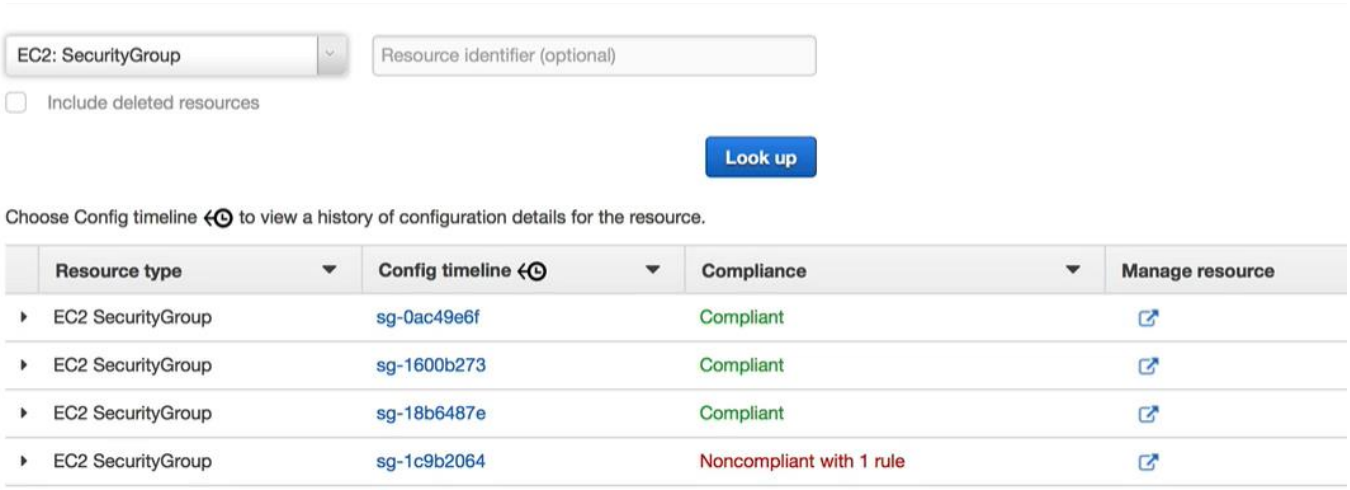

Рис.3.23 - Співставлення груп та правил

В таймлайні видно, яким змінам піддавалась група за весь час та які віртуальні машини були асоційовані з даною групою, як це зображено на рисунку 3.24.

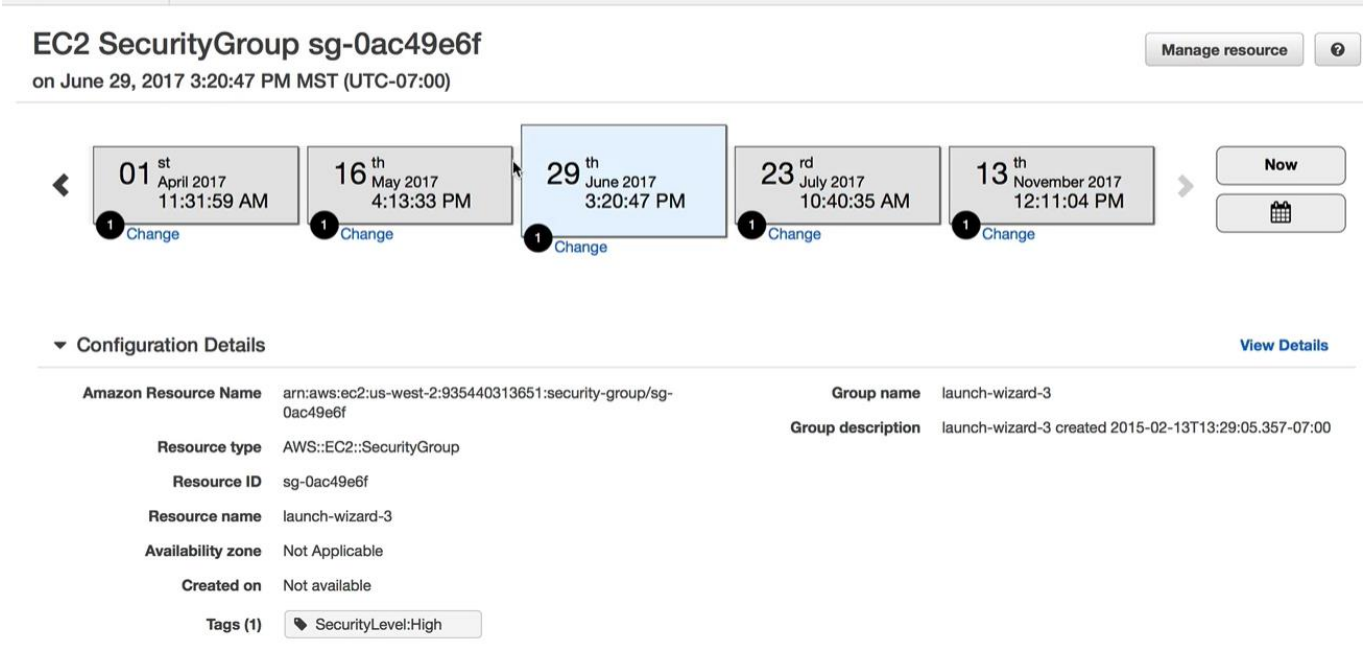

Рис.3.24 – Історія змін в групі безпеки

Висновки за розділом 3

У даному розділі було проведено ряд досліджень та отримано наступні практичні результати:

1. Вибрано найпопулярнішу архітектуру для хмарних обчислень та її налаштування Проведено аналіз існуючих рішень для впровадження технології керування обліковими записами
2. Написано власну політику безпеки для окремої групи
3. Запропоновано рішення для впровадження систем реагування на інциденти
4. Побудовано модель архітектури якісного сервісу із найбільш значущими компонентами для безпеки, моніторингом, інтерапарабельності та відмовостійкості роботи.
5. Наведено практичні рекомендації відносно коректного налаштування хмарного сховища для максимально ефективного використання хмари без надлишкового навантаження.

ВИСНОВКИ

У дипломній роботі розв’язано актуальне завдання створення безпечної хмарної архітектури. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено аналіз поширених загроз безпеки та аспектів, які є особливо схильними до атак та створюють особливу групу ризику. За результатами проведених досліджень було змодельовано безпечну хмарну архітектуру.

2. Обґрунтовано значущість та актуальність проблеми захисту даних в хмарі. Проаналізовано сервіси, які слід імплементувати в існуючу інфраструктуру задля забезпечення надійного рівня захисту.

3. Формалізовано задачу виявлення та локалізації інцидентів інформаційної безпеки у контексті створення комплексної системи захисту та контролю даних.

4. Розроблено та запропоновано оптимальну конфігурацію системи на основі хмарного провайдера Amazon.

5. Сформовано практичні рекомендації відносно здійснення налаштувань системи відповідно до технологічних та нормативних вимог безпеки, а також задля оптимального використання технологічного ресурсу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fesenko, A., Hlazkova, O. Security issues of software as a service (SaaS), infrastructure (IaaS) and Private Cloud/ Andriy Fesenko, Olena Hlazkova // PCSITS. – Kyiv, 2021.

2. Cloud Computing Stats - Security and Recovery [Електронний ресурс] – Режим доступу до ресурсу: https://www.slideshare.net/rapidscale/cloud-computing-stats-security-and-recovery.

3. 12 Benefits of Cloud Computing [Електронний ресурс] – Режим доступу до ресурсу: Cloud Computing Stats - Security and Recovery [Електронний ресурс] – Режим доступу до ресурсу: https://www.slideshare.net/rapidscale/cloud-computing-stats-security-and-recovery.

4. What is SDN and where software-defined networking is going [Електронний ресурс] – Режим доступу до ресурсу: https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html.

5. Software-defined network [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html#~what-is-sdn.

6. Blast Radius [Електронний ресурс] – Режим доступу до ресурсу: https://kemptechnologies.com/glossary/blast-radius/.

7. Cloud Security Best Practice: Limit Blast Radius with Multiple Accounts [Електронний ресурс] – Режим доступу до ресурсу: https://securosis.com/blog/cloud-security-best-practice-limit-blast-radius-with-multiple-accounts.

8. Security groups for your VPC [Електронний ресурс] – Режим доступу до ресурсу: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html.

9. Configuring Security Groups and Network ACLs [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/281643120_Using_the_Cloud_to_Teach_Computer_Networks#pf4.

10. RBAC vs. ABAC: What’s the Difference? [Електронний ресурс] – Режим доступу до ресурсу: https://www.dnsstuff.com/rbac-vs-abac-access-control#:~:text=The%20primary%20difference%20between%20RBAC,Essentially%2C%20when%20considering%20RBAC%20vs.

11. Malware Used by China APT Group Abuses Dropbox [Електронний ресурс] – Режим доступу до ресурсу: http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox.

12. Zepto variant of Locky ransomware delivered via popular Cloud Storage apps [Електронний ресурс] – Режим доступу до ресурсу: https://resources.netskope.com/h/i/273457617-zepto-variant-oflocky-ransomware-delivered-via-popular-cloud-storage-apps.

13. CloudSquirrel Malware Squirrels Away Sensitive User Data Using Popular Cloud Apps [Електронний ресурс] – Режим доступу до ресурсу:https://resources.netskope.com/h/i/272453388-cloudsquirrelmalware-squirrels-away- sensitive-user-data-using-popular-cloud-apps.

14. CloudFanta Pops with the Cloud using SugarSync [Електронний ресурс] – Режим доступу до ресурсу: https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-usingsugarsync.

15. Data Theft Via the Cloud: You Don’t Need Flash Drives Any More [Електронний ресурс] – Режим доступу до ресурсу: https://blog.learningtree.com/data-theft-via-cloud-dont-need-flash-drives/.

16. What Is Cloud DLP? [Електронний ресурс] – Режим доступу до ресурсу: https://digitalguardian.com/blog/what-cloud-dlp.

17. Best Practices for Cloud Security [Електронний ресурс] – Режим доступу до ресурсу: https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html.

18. Open, Vulnerable Containers Found Exposed on the Net [Електронний ресурс] – Режим доступу до ресурсу: https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-thenet/132898/.

19. Five Ways Shadow IT in the cloud hurts your enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://www.networkworld.com/article/2997152/cloud-computing/five-ways-shadow-itin-the-cloud-hurts-your-enterprise.html.

20. Cloud Adoption and Risk Report [Електронний ресурс] – Режим доступу до ресурсу: https://info.skyhighnetworks.com/WPCARR-Q2-2015_Download_White.html?Source=website&LSource=website.

21. Why Cloud Security Is Everyone's Business [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/.

22. Source: Deloitte Breach Affected All Company Email, Admin Accounts [Електронний ресурс] – Режим доступу до ресурсу: https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-allcompany-email-admin-accounts/.

23. Deloitte hack hit server containing emails from across US government [Електронний ресурс] – Режим доступу до ресурсу: https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hitserver-containing-emails-from-across-us-government.

24. Deloitte Gets Hacked: What We Know So Far [Електронний ресурс] – Режим доступу до ресурсу: http://fortune.com/2017/09/25/deloitte-hack.

25. "Get Off of My Cloud": Cloud Credential Compromise and Exposure [Електронний ресурс] – Режим доступу до ресурсу: https://www.defcon.org/images/defcon-19/dc-19-presentations/Feinstein.

26. Netflix Cloud Security: Detecting Credential Compromise in AWS [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/netflix-techblog/netflix-cloud-security-detecting-credentialcompromise-in-aws-9493d6fd373a.

27. Microsoft Security Intelligence Report [Електронний ресурс] – Режим доступу до ресурсу: https://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf.

28. Microsoft warns that hackers are increasingly targeting cloud accounts [Електронний ресурс] – Режим доступу до ресурсу:

https://www.theinquirer.net/inquirer/news/3016031/microsoft-warnsthat-hackers-are-increasingly-targeting-cloud-accounts.

29. Microsoft Security Intelligence Report volume 23 is now availablePoorlysecured CloudApps [Електронний ресурс] – Режим доступу до ресурсу: https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-reportvolume-23-is-now-available/.

30. Understand top trends in the threat landscape [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/sir.

31. What Is Amazon EC2? [Електронний ресурс] – Режим доступу до ресурсу: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/building-shared-amis.html.

32. Virtual machine prerequisites [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/azure/marketplace/cloud-partner-portal/virtual-machine/cpp-prerequisites.

33. How to Log a Security Event Support Ticket [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/azure/security/azure-security-event-support-ticket.