ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ХМАРНИХ СЕРВІСІВ ІЗ ВИКОРИСТАННЯМ CISCO STEALTHWATCH CLOUD»

Виконала студентка 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Васецька П. О.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. На сьогоднішній день хмарні сервіси є невід'ємною частиною інфраструктури багатьох компаній, що дозволяє їм швидко й ефективно обробляти дані та програми, зменшуючи витрати на обслуговування власних серверів. Майже всі сучасні продукти, від провідних лідерів до тільки-но створених, користуються хмарним середовищем. Оскільки збереження та обробка даних, резервне копіювання, розробка та тестування програмного забезпечення, віртуалізація серверів, робота з дистанційними робітниками тощо. Хмарне середовище може бути використано для ряду цілей, залежно від потреб користувача та бізнес-задач.

Однак, як і будь-яка інша технологія, хмарні сервіси також можуть стати об'єктом кібератак і порушень конфіденційності даних. Щоб забезпечити захист хмарних сервісів, компанії повинні використовувати різноманітні засоби безпеки, включаючи інтегровану в хмару систему безпеки Cisco Stealthwatch.

З огляду на низку переваг, які пропонує хмара, безпека даних є однією з ключових проблем, які стримують підприємства від впровадження хмарних рішень. Компанії помірно або надзвичайно стурбовані ризиками безпеки хмарних обчислень.

Хмарна інфраструктура може бути складною, що складність є ворогом безпеки. Незважаючи на те, що більшість експертів із хмарної безпеки сходяться на думці, що компанії можуть отримати вигоду від рішень безпеки, вбудованих у хмару, організації також можуть допускати серйозні помилки та викривати критичні дані та системи.

Також однією з найважливіших проблем, пов'язаних із безпекою хмарних служб, є відсутність повного контролю над даними та програмами, що зберігаються на віддалених серверах. Це створює значний ризик для безпеки даних компанії, оскільки дозволяє злочинцям отримати несанкціонований доступ до даних та інформації користувачів.

Актуальність цієї роботи пояснюється необхідністю гарантувати, що передача, обробка та зберігання даних користувачів за допомогою хмарних технологій забезпечує належний рівень захисту даних користувачів відповідно до їх класифікації.

Метою роботи є дослідження методів і покращення засобів захисту інформації та розробка моделі системи захисту інформації для хмарної СУБД, яка дозволить побудувати та забезпечити належний рівень безпеки даних шляхом оптимізації використання ресурсів для функціонування інформаційної системи.

Об'єкт дослідження — хмарні середовища.

Предмет дослідження — захист хмарних середовищ з використанням Cisco Stealthwatch Cloud

Мета роботи — дослідити можливості захисту хмарних середовищ з використанням Cisco Stealthwatch Cloud та розробити рекомендації щодо покращення ефективності захисту.

Методи дослідження — аналіз технічних можливостей Cisco Stealthwatch Cloud, вивчення принципів захисту хмарних середовищ, проведення огляду на тестових середовищах, як наслідок цього аналіз результатів тестування та розробка рекомендацій

1 АНАЛІЗ ВПЛИВУ ВРАЗЛИВОСТЕЙ НА ХМАРНІ СЕРВІСИ

1.1 Необхідність захисту хмарних сервісів

У світі мультихмарних технологій IT-менеджери швидко усвідомлюють переваги послуг хмарних обчислень таких як інфраструктура як послуга. Захист хмарних сервісів є надзвичайно важливим у зв'язку зі зростанням об'ємів даних, які зберігаються в хмарі. Хмарні сервіси можуть бути скомпрометовані різними способами, включаючи злам паролів, викрадення ідентифікаторів користувача, крадіжку даних, введення в систему шкідливого коду, розповсюдження зловмисних програм та інших видів кіберзлочинності.

Основна необхідність захисту хмарних сервісів полягає в тому, щоб забезпечити безпеку даних та забезпечити можливість їх безпечної обробки.

Хмарні архітектури не є стандартизованими, і кожен постачальник хмарних послуг (ПХП) реалізує основні хмарні сервіси по-різному. Розуміння того, як провайдер реалізує хмарні сервіси, повинно бути частиною рішення про ризики, яке приймає клієнт під час закупівлі хмарних послуг хмарних сервісів. Чотири хмарні архітектурні сервіси є спільними для більшості хмар.

Але розглянемо декі компоненти хмари:

Управління ідентифікацією та доступом (IdAM). IdAM відноситься до засобів контролю, що застосовуються клієнтами для захисту доступу до їхніх ресурсів, а також до засобів контролю, що застосовуються ресурсів, а також засоби контролю, які використовує CSP для захисту доступу до внутрішніх хмарних ресурсів. Захист клієнта IdAM для клієнтів і внутрішніх хмарних ресурсів, як впровадження, так і аудит, має вирішальне значення для захисту хмарних ресурсів клієнтів.

Обчислення. Хмари зазвичай покладаються на віртуалізацію та контейнеризацію для управління та ізоляції обчислювальних робочих навантажень клієнтів. Безсерверні обчислення, динамічний розподіл хмарних обчислювальних

ресурсів для виконання клієнтського коду, побудовані на віртуалізації або контейнеризації, залежно від хмарного сервісу.

- *Віртуалізація* є базовою технологією хмарних обчислень не лише для робочих навантажень клієнтів, але й для самої хмарної хмарної архітектури. Віртуалізація - це технологія, яка забезпечує ізоляцію в хмарі як для як для сховища, так і для мережі. Віртуалізація зазвичай реалізує та захищає внутрішні хмарні вузли.
- *Контейнеризація* - це більш легка технологія, яка зазвичай використовується в хмарах для управління та ізоляції робочих навантажень клієнтів. Контейнеризація є менш безпечною технологією ізоляції, ніж віртуалізація через спільні характеристики ядра, але CSP пропонують технології, які допомагають усунути недоліки безпеки контейнеризації.

Ізоляція мереж клієнтів є критично важливою функцією безпеки хмари. Крім того, хмарна мережа повинна впроваджувати засоби контролю по всій хмарній архітектурі, щоб захистити хмарні ресурси клієнтів від внутрішніх загроз. Програмно-визначені мережі зазвичай використовуються в хмарі як для логічного розділення мереж клієнтів, так і для як для логічного розділення мереж клієнтів, так і для реалізації магістральної мережі для хмари.

Сховище (об'єкти, блоки та записи в базі даних). Дані клієнта логічно відокремлені від інших даних клієнта даних клієнтів у хмарних вузлах. Повинні існувати механізми безпеки, щоб гарантувати, що дані клієнта не витікають до інших клієнтам, а також захистити дані клієнта від внутрішніх загроз.

Хмарне шифрування та управління ключами. Хоча шифрування та управління ключами (КМ) не є базовим компонентом хмарних архітектур, вони є важливим аспектом захисту інформації в хмарі, захисту інформації в хмарі. Хоча CSP використовує шифрування (серед інших засобів контролю) для захисту деяких аспектів даних клієнтів від інших клієнтів і співробітників CSP, клієнти хмарних сервісів повинні розуміти, які можливості вони мають для подальшого захисту своїх даних. Розуміння вимог до чутливості даних має вирішальне значення для побудови хмарного шифрування та ключової стратегії управління.

1.2 Аналіз вразливостей хмарних середовищ

Хмарні вразливості поділяються на чотири класи (неправильна конфігурація, поганий контроль доступу, вразливості спільного використання та вразливості ланцюжка постачання), які охоплюють переважну більшість відомих вразливостей. Користувачі хмарних сервісів клієнти відіграють важливу роль у зменшенні впливу неправильної конфігурації та поганого контролю доступу, але вони також можуть вжити заходів для захисту хмарних ресурсів від використання вразливостей спільної оренди та ланцюгів постачання.

Неправильно налаштоване хмарне сховище. Хмарне сховище є багатим джерелом викрадених даних для кіберзлочинців. Незважаючи на високі ставки, організації продовжують робити помилку неправильної конфігурації хмарного сховища, яка коштує багатьом компаніям дуже дорого.

Неправильна конфігурація хмарного сховища може швидко перерости в серйозне порушення безпеки хмари для організації та її клієнтів. Нажаль, широко розповсюджена, через низьку складність для зловмисника. Хоча переважно зазвичай надаються інструменти для управління конфігурацією хмари, але неправильна конфігурація хмарних ресурсів залишається найпоширенішою вразливістю хмари, яка може бути використана для доступу до хмарних даних і сервісів. Помилки в хмарних сервісах, що часто виникають через політики хмарних сервісів або нерозуміння спільної відповідальності, неправильна конфігурація має наслідки, які варіюються від відмови в обслуговуванні до вразливості облікових записів до компрометації облікових записів. Швидкі темпи інновацій CSP створюють нові функціональні можливості, але також додають складність безпечного налаштування хмарних ресурсів організації. Є кілька типів неправильних конфігурацій хмари, з якими стикаються підприємства. Деякі типи неправильних конфігурацій включають:

Неправильна конфігурація групи безпеки AWS. Групи безпеки AWS відповідають за забезпечення безпеки на рівнях доступу джерела, призначення, порту та протоколу. Вони можуть бути пов’язані з примірниками сервера та

багатьма іншими ресурсами. Неправильна конфігурація в групах безпеки AWS може дозволити зловмиснику отримати доступ до ваших хмарних серверів і викрасти дані.

Відсутність обмежень доступу. Неадекватні обмеження або засоби захисту для запобігання несанкціонованому доступу до вашої хмарної інфраструктури можуть поставити ваше підприємство під загрозу. Незахищені сегменти хмарного сховища можуть призвести до того, що зловмисники отримають доступ до даних, що зберігаються в хмарі, і завантажать конфіденційні дані, що може мати руйнівні наслідки для вашої організації. AWS спочатку мав відкриті сегменти S3 за замовчуванням, і це призвело до безлічі порушень даних.

Поганий контроль доступу. Також один з поширених вразливостей у сферізахисту хмарних середовищ. Поганий контроль доступу виникає, коли хмарні ресурси використовують слабкі методи автентифікації/авторизації або містять вразливості, які обходять ці методи. Слабкість механізмів контролю доступу може дозволити зловмиснику підвищити привілеї, що призведе до компрометації хмарних ресурсів. Інтерфейс користувача програми (API) призначений для оптимізації процесів хмарних обчислень. Однак, якщо API залишаються незахищеними, вони можуть відкривати лінії зв’язку для зловмисників, щоб використовувати хмарні ресурси.

Зі збільшенням залежності від API зловмисники знайшли звичайні способи використовувати незахищені API для зловмисних дій.

- Некоректна автентифікація: часто розробники створюють API без належного контролю автентифікації. У результаті ці API повністю відкриті для Інтернету, і будь-хто може використовувати їх для доступу до корпоративних даних і систем.
- Некоректна авторизація: надто багато розробників вважають, що зловмисники не побачать виклики серверного API, і не встановлюють відповідні елементи керування авторизацією. Якщо цього не зробити, компрометація серверних даних є тривіальною.

Вразливості спільного використання. Не поширене, через складність виконання, але вразлтвість існує, як наслідок є ризики. Хмарні платформи складаються з безлічі програмних і апаратних компонентів. Зловмисники, які можуть визначити програмне або апаратне забезпечення, що використовується в хмарній архітектурі, можуть скористатися вразливостями для підвищення привілеїв у хмарі. Вразливості в хмарних гіпервізорах (тобто програмному/ апаратному забезпеченні, яке забезпечує віртуалізацію) або контейнерних платформах є особливо серйозні через критичну роль, яку ці технології відіграють у захисті хмарних архітектур та ізоляції клієнтських робочих навантажень клієнтів. Вразливості гіпервізорів складно і дорого виявити і використати, що обмежує їх використання просунутими зловмисниками. Також відстежуються системні журнали на наявність будь-яких ознак використання гіпервізора. Контейнеризація, хоча і є привабливою технологією з точки зору продуктивності та портативності, повинна бути ретельно обміркована перед розгортанням у багатокористувацькому середовищі. Контейнери працюють на спільному ядрі, без рівня абстракції, який забезпечує який забезпечує віртуалізація. У багатокористувацькому середовищі, такому як хмара, вразливість контейнерної платформи може дозволити зловмиснику скомпрометувати контейнери інших користувачів на тому ж хості.

Втрата або викрадення інтелектуальної власності. Інтелектуальна власність (IP), безсумнівно, є одним із найцінніших активів організації, а також вразлива до загроз безпеці, особливо якщо дані зберігаються в Інтернеті. Для багатьох організацій IP – це дані, якими вони володіють, і втрата даних означає втрату IP-адреси. Давайте розглянемо найпоширеніші причини втрати даних:

Зміна даних. Коли дані певним чином змінені та їх неможливо відновити до попереднього стану, це може призвести до втрати повної цілісності даних і зробити їх марними.

Видалення даних. Зловмисник може видалити конфіденційні дані з хмарної служби, що, очевидно, створює серйозну загрозу безпеці даних для операцій організації.

Втрата доступу. Зловмисники можуть зберігати інформацію з метою отримання викупу (атака програм-вимагачів) або шифрувати дані за допомогою надійних ключів шифрування, доки не виконають свої зловмисні дії.
Тому важливо вживати превентивних заходів для захисту вашої інтелектуальної власності та даних у хмарному середовищі.

Вразливості ланцюжка постачання. Вразливості ланцюжка поставок у хмарі включають наявність внутрішніх зловмисників та навмисні бекдори в апаратному та програмному забезпеченні. CSP постачають апаратне та програмне забезпечення з усього світу і наймають розробників багатьох національностей.

Сторонні програмні хмарні компоненти можуть містити вразливості, навмисно вставлені розробником, щоб скомпрометувати програму. Впровадження агента в хмарний ланцюжок поставок, як постачальника, адміністратора або розробника, може бути ефективним засобом для зловмисників національних держав ефективним засобом для зловмисників з національних держав скомпрометувати хмарні середовища операцій та сповіщення про підозрілі дії адміністраторів.

1.3 Наявні методи захисту хмарних сервісів

Розглянемо детально деякі методи захисту хмарних сервісів:

Аутентифікація та авторизація. Це процеси, які дозволяють перевірити, чи є користувач, який намагається отримати доступ до хмарного сервісу, правомірним користувачем. Для цього, користувачі повинні використовувати сильні паролі та двофакторну аутентифікацію. Для забезпечення аутентифікації та авторизації в хмарному сервісі можуть використовуватися різні методи. Один з найпоширеніших методів – це використання ідентифікатора користувача та пароля. Користувач вводить свій ідентифікатор та пароль, які потім перевіряються хмарним сервісом для підтвердження його ідентичності та визначення прав доступу до сервісу. Інші методи аутентифікації та авторизації включають використання біометричних даних, токенів безпеки та систем одноразових паролів. Наприклад, біометрична

аутентифікація може використовувати відбитки пальців або розпізнавання обличчя для підтвердження ідентичності користувача, тоді як токени безпеки можуть надавати доступ до сервісу, якщо користувач має певний пристрій або картку доступу.

Контроль доступу. Важливий у сфері кібербезпеки процес, який дозволяє обмежити доступ користувачів до різних функцій та ресурсів хмарного сервісу. В собі має налаштування прав доступу, визначення ролей користувачів та встановлення політик безпеки. Оскільки, цей метод є не менш важливим, розглянемо детальніше різні методи контролю доступу, для забезпечення безпеки в хмарних середовищах. Основні з них: рольовий контроль доступу, політики контролю доступу, мультифакторна аутентифікація.

Рольовий контроль доступу (Role-Based Access Control, RBAC) – метод, за яким доступ до ресурсів надається на основі ролі, яку виконує користувач в організації. Доступ до ресурсів надається на основі списків ролей, які відповідають конкретним діям або обов'язкам. Ролі мають ієрархічну структуру, і доступ до ресурсів залежить від рівня ролі, яку має користувач.

Політики контролю доступу (Access Control Policies) – це набір правил, які визначають, які користувачі мають доступ до ресурсів, і які рівні доступу надаються. Політики контролю доступу можуть використовуватися для контролю доступу до файлів, баз даних, веб-сайтів і інших ресурсів. При створенні політик контролю доступу можуть використовуватися різні фактори, такі як ролі, групи, ідентифікатори користувачів, IP-адреси та інші.

Мультифакторна аутентифікація (Multi-Factor Authentication, MFA) – це метод, який використовує більше одного фактора аутентифікації, щоб забезпечити більш високий рівень безпеки. Наприклад, при вході в хмарний сервіс може бути вимаганий не тільки логін та пароль

Шифрування. Це процес перетворення звичайного тексту в криптографічно захищений текст, який може бути розшифрований лише за допомогою відповідного ключа. Також процес, який дозволяє зашифрувати дані на період їх передачі та зберігання в хмарному сервісі. Для цього використовуються різні алгоритми

шифрування, такі як AES, RSA, та інші. Шифрування в хмарних середовищах може бути здійснене на різних рівнях: на рівні даних, на рівні передачі даних та на рівні зберігання даних. На рівні даних, шифрування може бути використане для захисту конфіденційної інформації, яка зберігається в базі даних або на файловій системі. На рівні передачі даних, шифрування може бути використане для захисту інформації, яка передається по мережі, включаючи електронну пошту та інші комунікаційні протоколи. На рівні зберігання даних, шифрування може бути використане для захисту даних, які зберігаються в хмарних сховищах. Застосування шифрування в хмарних середовищах забезпечує більш високий рівень безпеки даних та зменшує ризик їх втрати чи крадіжки.

Моніторинг. Процес, який дозволяє відстежувати та аналізувати активність користувачів та даних в хмарному сервісі. Виконується з метою виявлення можливих загроз безпеці, а також для забезпечення дотримання правил та обмежень, пов'язаних зі зберіганням та обробкою даних у хмарі. Однією з ключових ролей моніторингу в безпеці хмарних середовищ є вчасне виявлення можливих загроз безпеці, таких як атаки хакерів, витоки даних або інші інциденти. За допомогою моніторингу можна відстежувати поведінку користувачів у хмарі, що дозволяє вчасно виявляти підозрілі дії та запобігати можливим загрозам.

Захист від шкідливого програмного забезпечення. Також варто зазначити, хоча цей процес суто індивідуальний для кожного підприєства, але досить важливий процес, який дозволяє виявляти та запобігати використанню шкідливого програмного забезпечення в хмарному сервісі. Для цього використовуються антивірусні програми, системи виявлення та інші діючі рішення.

Резервне копіювання. Ключовий елемент захисту, який дозволяє зберігати копії даних, що зберігаються в хмарному сервісі, щоб у разі втрати даних, їх можна було відновити. Для забезпечення ефективного резервного копіювання в хмарних середовищах необхідно використовувати сучасні рішення та мати надійні безпечні місця зберігання даних.

Віддалений доступ користувача. Ряд дій, які дозволяють користувачам отримувати доступ до хмарного сервісу з будь-якої точки світу. Для цього

використовуються захищені протоколи та віртуальні приватні мережі. В той же час, віддалений доступ може створювати певні ризики для безпеки даних і інфраструктури хмарного середовища. Тому створений ряд правил для забезпечення безпеки хмарного середовища з віддаленим доступом.

Система управління безпекою. Процес, який дозволяє керувати та контролювати всі аспекти безпеки хмарного сервісу. Він включає в себе встановлення політик безпеки, оцінку ризиків, аналіз вразливостей та інші функції. Основна роль якої, в беспеці хмарних середовищ полягає в тому, щоб забезпечити відповідний рівень захисту та безпеки для інформації, що зберігається в хмарі. Це досягається шляхом запровадження політик безпеки, забезпечення відповідності до них і контролю за їх виконанням.

Перевірка внутрішньої безпеки: це процес, який дозволяє виконувати перевірку на внутрішню рівні, полягає у виявленні потенційних загроз безпеці, які виникають зсередини організації, тобто з боку працівників, партнерів та інших осіб, які мають доступ до хмарних ресурсів. Це дозволяє організації ідентифікувати можливі ризики та вживати необхідних заходів для запобігання можливим інцидентам. В ролі перевірки внутрішньої безпеки можуть використовуватися такі методи, як моніторинг активності користувачів, аудит безпеки, аналіз журналів, сканування вразливостей, перевірка прав доступу та інші методи.

1.4 Відомі рішення для моніторингу мережі хмарних середовищ

Наведені рішення є лідируючими на ринку кібернетичної безпеки.

Cisco Stealthwatch Cloud — рішення для моніторингу безпеки мережі, яке використовується для виявлення та відповіді на кібератаки. Воно забезпечує підтримку різних типів мереж, включаючи хмарні середовища. Основна функція Cisco Stealthwatch Cloud – це забезпечення аналізу мережевого трафіку та виявлення аномалій у поведінці мережі. Він також забезпечує візуалізацію мережевого трафіку та здатність до детального аналізу кожного з'єднання в мережі. Також має широкий спектр функцій та можливостей, що дозволяє вирішувати

більшість проблем з безпекою мережі та захистити корпоративні ресурси від різних загроз в Інтернеті

SolarWinds Network Performance Monitor — це рішення, яке забезпечує повний огляд мережі хмарних сервісів, включаючи топологію мережі, швидкість передачі даних та різні метрики мережевої продуктивності, дозволяє відстежувати та аналізувати стан різних компонентів мережі, включаючи сервери, маршрутизатори, комутатори, мережеві принтери та інші пристрої. Це рішення може бути встановлено в хмарному середовищі або локально на пристрої з Windows або Linux. З переваг та можливостей даного продукту можна зазначити моніторинг мережевих пристроїв, серверів, додатків, аналіз мережі та автоматизованеуправління. І що не менш важливо простий інтерфейс з легким налаштуванням.

Zscaler Internet Access — це рішення, яке забезпечує безпеку в Інтернеті в хмарній моделі, де всі трафіки пересилаються через обліковий запис користувача в хмарі. Вона включає в себе функції контролю доступу, фільтрації вмісту, брандмауеру та інших безпекових функцій, пропонує захист від загроз, контроль доступу та реалізацію політик безпеки для користувачів і пристроїв, що працюють за межами корпоративної мережі. Деякі з можливостей та переваг даного продукту можна зазначити у безпечному доступу до Інтернету, захисту від шкідливих веб-сайтів, фішингу, вірусів та інших загроз, контролі доступу, впровадженні та реалізації політик безпеки, захисту конфіденційної інформації шляхом скасування зберігання даних на пристроях користувачів.

Palo Alto Networks Prisma Access — це рішення, яке рішення з захисту хмарних сервісів, яке забезпечує безпечний доступ до хмарних додатків та сервісів для користувачів, які працюють з різних місць та на різних пристроях. Prisma Access використовує технологію SASE (Secure Access Service Edge), яка поєднує в собі функції мережевої безпеки та контролю доступу до додатків, що дозволяє забезпечити безпеку користувачів в будь-якому місці та на будь-якому пристрої, що комбінує функції безпеки та мережевої продуктивності в хмарі. З його переважного функціоналу можна зазначити такі основні сожливості: забезпечення

гнучкого контролю доступу до хмарних додатків, що дозволяє обмежити доступ до них лише авторизованим користувачам та пристроям, також рішення використовує мережеві та безпекові функції для захисту користувачів від шкідливих програм та загроз дозволяє користувачам отримувати доступ до хмарних додатків з будь-якого місця та на будь-якому пристрої, забезпечує централізоване керування та моніторинг доступу до хмарних додатків, дозволяє користувачам швидко та безпечно отримувати доступ до хмарних додатків, що дозволяє підвищити продуктивність праці.

Fortinet FortiGate — це рішення, яке забезпечує широкий спектр функцій безпеки мережі в хмарі, включаючи захист від загроз, мережевий брандмауер, контроль доступу та VPN, захисту від DDoS-атак та інших функцій. З основних його переваж можна виділити те, що Fortinet FortiGate підтримує швидкості від 20 Мбіт/с до 1 Тбіт/с, що дозволяє йому відповідати на потреби різних типів мереж, має інтелектуальний контроль доступу, який дозволяє обмежувати доступ до мережевих ресурсів залежно від часу, місця та пристрою користувача, підтримує різні методи шифрування, такі як AES, SSL і IPSec, для захисту мережевого трафіку від перехоплення та розшифрування, підтримує централізоване управління, що дозволяє керувати всіма пристроями FortiGate з однієї точки, забезпечує захист мережі від надмірного трафіку, що може призвести до відмови в обслуговуванні і звичайно ж, моніторингу мережі, яка дозволяє виявляти та локалізувати проблеми мережі, такі як затори та відмови, та допомагає вирішувати їх.

1.5 Обов’язкові фунції для програмного забезпечення моніторингу хмарного сервісу

Швидке та просте розгортання. За визначенням, програмна платформа безпеки в хмарі має бути легкою для розгортання. На відміну від повністю налаштованого рішення, яке об’єднує інструменти різних постачальників, фірмові сервіси та інтеграцію, ці платформи готові до використання одразу. Вкладіть кошти в пробний період і розробіть угоду про рівень обслуговування (SLA) зі своїм

постачальником, щоб ви могли бачити точні терміни розгортання та потреби в зусиллях (як для вашої внутрішньої команди, так і для підтримки постачальника).

Збір та аналіз даних. Система повинна збирати дані з усіх джерел в мережі та аналізувати їх для виявлення проблем та потенційних загроз безпеці, відіграють ключову роль в рішеннях для моніторингу мережі хмарних сервісів. Ці рішення зазвичай збирають інформацію про різні параметри мережі, такі як пропускна здатність, завантаження, пристрої, які підключені до мережі, та багато іншого. Збір та аналіз цих даних дозволяє адміністраторам мережі відстежувати рівень продуктивності мережі та виявляти проблеми, які можуть виникати. Наприклад, адміністратор може виявити, що певний пристрій в мережі завантажується надмірно, і прийняти заходи для зменшення навантаження на цей пристрій.

Виявлення загроз. Рішення повинно мати здатність виявляти потенційні загрози для мережі, в тому числі шкідливі програми, вторгнення та злочинну діяльність. Для забезпечення безпеки мережі, система моніторингу повинна бути здатна реагувати на потенційні загрози. Для цього різні рішення для моніторингу мережі хмарних сервісів зазвичай використовують методи виявлення загроз базуючись на потребах підприємства: поведінковий аналіз, аналіз стану мережі, визначені сигнатури атак для виявлення шкідливих пакетів.

Моніторинг мережевої пропускної здатності: система моніторингу повинна мати здатність аналізувати використання пропускної здатності та ідентифікувати будь-які проблеми з її використанням. допомагає ідентифікувати проблеми зі збільшенням трафіку в мережі та відслідковувати, які додатки можуть бути винуватцями цих проблем. Крім того, ця функція може бути використана для виявлення джерела надмірного трафіку та зменшення його впливу на мережу.

Моніторинг мережевої доступності. Також одна з основних компонентів, що забезпечує доступність хмарних сервісів для користувачів шляхом постійного моніторингу стану мережевого з'єднання між користувачами та хмарним сервісом. Моніторинг мережевої доступності також дозволяє визначити, які сервіси використовують більше всього мережевої пропускної здатності, та забезпечує контроль за її використанням.

Візуалізація даних: система моніторингу повинна надавати користувачеві зручні інструменти для візуалізації даних про мережу, щоб допомогти приймати рішення щодо її управління та оптимізації. Вона полягає в тому, щоб забезпечити користувачам зручний і швидкий доступ до даних про стан мережі та сервісів, допомагає відслідковувати тенденції, виявляти аномальні поведінки та проблеми.

Забезпечення безпеки. Система моніторингу повинна мати вбудовані функції захисту від потенційних загроз, таких як вторгнення та зловмисні програми повинні мати вбудовані заходи безпеки, які забезпечують захист від загроз, таких як атаки DDoS, вторгнення, зловживання привілеями та інші. Безпека також охоплює захист від зловмисників, які можуть намагатися зламати паролі або скористатися іншими методами для отримання доступу до мережі.

Підтримка та розширюваність. Рішення повинно бути легко розгорнути та підтримувати, а також бути гнучким та можливим до розширення в разі зростання масштабів мережі, підтримки нових функцій та можливостей, а також швидкого відгуку на помилки та проблеми. Це може бути досягнуто шляхом використання модульної архітектури, що дозволяє додавати нові функції та підтримку нових протоколів без значних змін у системі моніторингу.

Інтеграція з іншими системами. Більшість компаній мають декілька різних систем для керування інфраструктурою, таких як системи управління конфігураціями, системи керування журналами подій, системи моніторингу безпеки та інші. Інтеграція рішень моніторингу мережі хмарних сервісів з цими системами може допомогти забезпечити більш повне розуміння стану мережі та забезпечити більш ефективний процес управління.

1.6 Статистика інцидентів хмарних середовищ

Підтримка безпеки в мультихмарному середовищі : звіт Radware показав, що, незважаючи на використання різноманітних інструментів безпеки для захисту своїх хмарних програм, 70% організацій не впевнені у своїй здатності підтримувати узгоджені заходи безпеки в локальному та багатохмарному середовищах.

Порушення даних у багатохмарних мережах: 69% опитаних організацій зізналися, що стикалися з порушеннями даних або розкриттям даних через багатохмарні конфігурації безпеки.

Найбільша перешкода безпеці в мультихмарному середовищі: основною перешкодою для захисту багатохмарних середовищ у 2022 році була визначена відсутність досвіду в розгортанні та управлінні комплексним рішенням у всіх хмарних середовищах.

Крім того, значні 37% респондентів у всьому світі повідомили, що їхні організації стикаються з труднощами, щоб не відставати від темпів змін, коли мова йде про безпеку багатохмарних середовищ.

Основні виклики хмарної безпеки, з якими стикаються організації, змінилися за останнє десятиліття: управління витратами на хмару (82%) обійшло безпеку (79%) і претендувало на перше місце. Цю зміну пріоритетів можна пояснити тим фактом, що організації здобули більше впевненості в заходах захисту хмари, що призвело до більшого впровадження хмарних служб і, як наслідок, до збільшення витрат на хмару.

Доповідь розширюється до дев’яти різних відомих викликів хмарній безпеці, з якими стикаються всі організації, які брали участь в опитуванні:

- Управління витратами на хмару (82%)
- Безпека (79%)
- Брак ресурсів/експерту (78%)
- Управління (71%)
- Відповідність (73%)
- Керування ліцензіями на програмне забезпечення (72%)
- Хмарна міграція (66%)
- Баланс відповідальності центральної хмарної команди/бізнес-підрозділу (67%)
- Управління мультихмарою (66%)

Комплексна хмарна стратегія, яка вирішує ці проблеми, може допомогти організаціям розкрити весь потенціал хмари, одночасно забезпечуючи безпеку та економічну ефективність.

Але чим більше популіризована хмара тим більше вона стає головним приорітетом у кіберзлочинців. Приблизно половина всіх витоків даних відбувається в хмарі.

Незважаючи на те , що 45% витоків даних відбулося в хмарі, організації, які використовують підхід гібридної хмари, зазнали нижчих середніх витрат на витік даних на рівні 3,80 мільйонів доларів США порівняно з організаціями, які використовували виключно публічні або приватні хмарні моделі. За даними IBM, середня вартість витоку даних в організаціях, які використовують приватну хмару, становить 4,24 мільйона доларів США . Згідно зі звітом Snyk, 80% організацій зіткнулися зі значним інцидентом безпеки, пов’язаним з їх хмарною інфраструктурою, протягом останнього року.

Основні хмарні інциденти:

- Порушення хмарних даних (33%)
- Витік даних у хмарі (28%)
- Порушення навколишнього середовища (27%)
- Криптомайнінг (23%)
- Серйозне порушення комплаєнсу (25%)
- Невдалий аудит (15%)
- Простой системи через неправильну конфігурацію (34%)

Організації з високорозвиненою хмарною безпекою вважають виявлення неправильних конфігурацій у хмарі своїм головним пріоритетом .

Насправді неправильна конфігурація хмарних ресурсів є основною проблемою для будь-якої організації, яка використовує хмарні служби. Ці помилки зазвичай трапляються, коли організації налаштовують і розгортають свою хмарну інфраструктуру, використовуючи консолі або інфраструктуру хмарних провайдерів як код.

Звіт Check Point про хмарну безпеку за 2022 рік показав, що 27% компаній зіткнулися з порушенням безпеки у своїй публічній хмарній інфраструктурі за останній рік. Серед цих інцидентів майже чверть (23%) були спричинені неправильною конфігурацією безпеки хмарної інфраструктури.

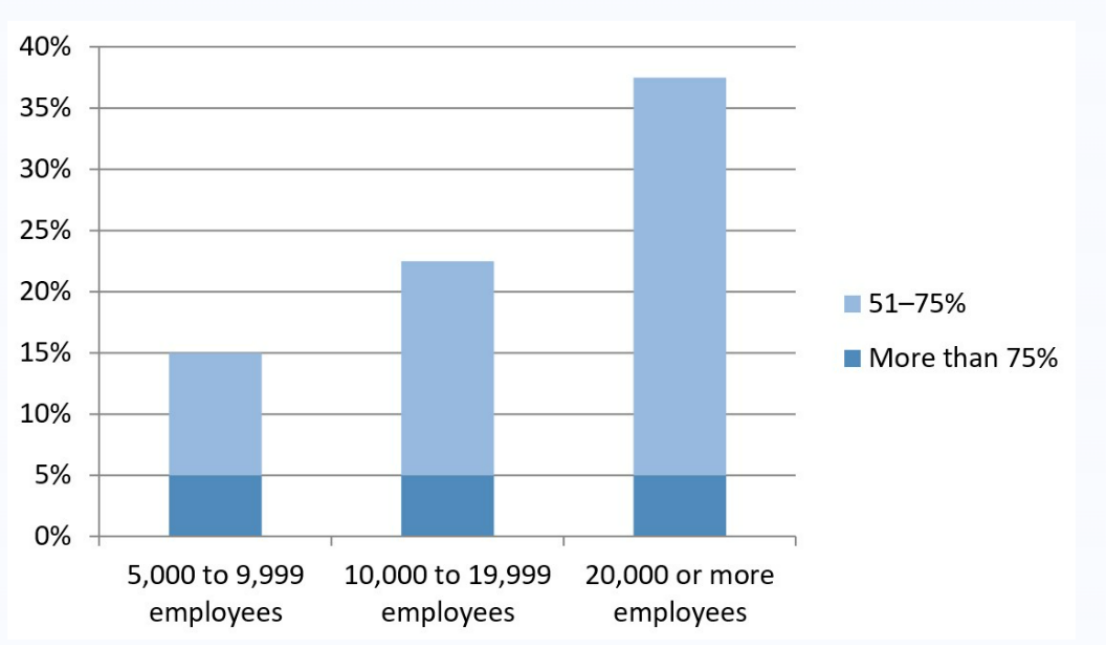

Рис.1.1. Частка порушень доступу до хмарних даних за розміром компанії

Основний ризик виникає через комбінацію помилок, зроблених під час розгортання, і неавторизованих змін, внесених після розгортання, що може призвести до різних інцидентів безпеки хмари. Дуже важливо бути проактивним у моніторингу та управлінні хмарними конфігураціями, щоб запобігти ризикам безпеки та захистити конфіденційні дані.

Інциденти безпеки хмари поширюються на різні частини хмари. Дослідження, проведене компанією Synk, показує деякі з основних напрямків, а саме:

- Неправильна конфігурація IAM (17%)
- Неправильна конфігурація зберігання об'єктів (20%)
- Небезпечне використання резервних копій даних (23%)
- Незахищені ключі API (20%)
- Відсутність моніторингу (20%)

Той факт, що так багато компаній повідомляють про те, що їхні конфіденційні дані були розкриті в хмарі, і вказують на доступ як основну причину порушень хмарних даних, додатково відображається на основних драйверах керування дозволами доступу до хмарної інфраструктури. У всій вибірці опитування організації назвали збереження конфіденційності конфіденційних даних у хмарі від внутрішніх загроз (це вибрано 58% респондентів) і від зовнішніх атак і несанкціонованого доступу (57%) як основні такі фактори.

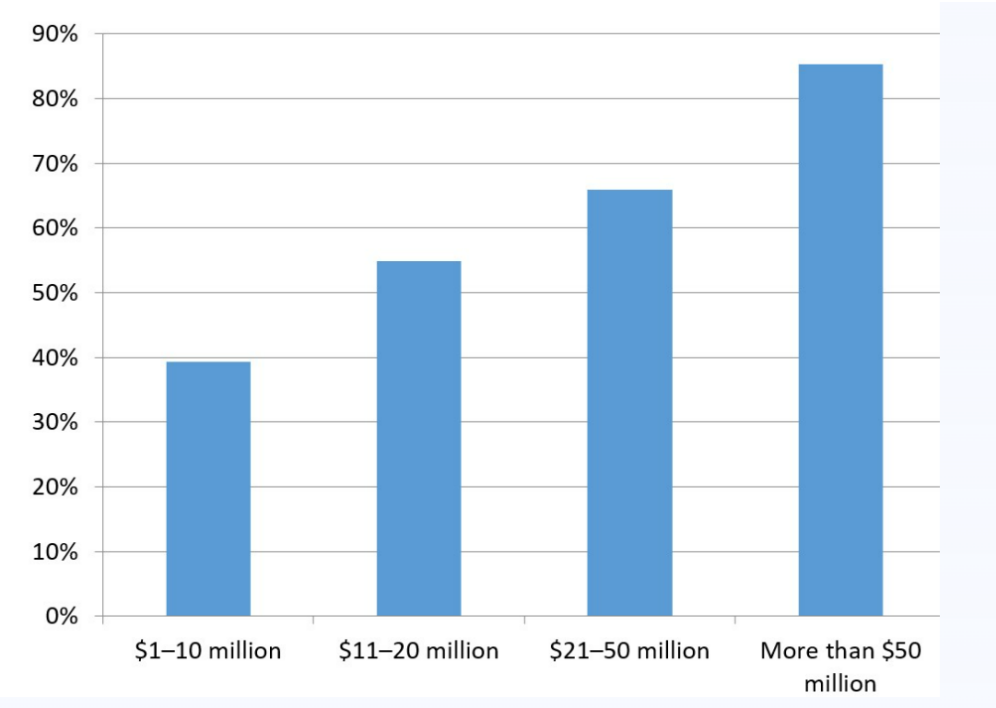

Рис.1.2. Вплив на витоки конфіденційних даних через хмарний слід

Висновки до першого розділу

Визначено, які є вразливості хмарних середовищ, навіщо підприємствам їх захист та які можуть бути наслідки за відсутності. Також було розглянуто основні та обов’язкові вимоги для програмного забезпечення зля захисту хмарних середовищ. Зазначено зростання вразливостей зі збільшенням підприємства.

Простежено, що більшість порушень спричинені саме людським фактором та недооцінення ризиків, що призводить на даний час дуже великі збитки.

Проаналізовано більший контроль робітників та їх кваліфікація шляхом посилення політик безпеки та їх дотримання.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БОРОТЬБИ З ВРАЗЛИВІСТЯМИ

2.1 Визначення найбільш поширених видів атак на хмарні сервіси та їхніх наслідків

Поширені атаки на хмарну безпеку для хмарних обчислень:

У сучасних технологіях хмарні технології відкрили абсолютно нові можливості для зберігання, доступу, гнучкості та продуктивності, що посилило новий світ проблем безпеки. SaaS, PaaS та IaaS також розкривають питання інформаційної безпеки та ризики хмарних обчислювальних систем. Хоча хмарні обчислення можуть розглядатися як вирішення всіх проблем, але, незважаючи на їхні переваги, вони мають низку суттєвих недоліків, які слід взяти до уваги. Перенесення корпоративних IT у хмару - це складне завдання, яке включає в себе як технічні, так і організаційні проблеми, як технічного, так і організаційного характеру.

Деякі основні проблеми безпеки хмарних сервісів:

Витоки даних. Визначається як витік конфіденційних даних клієнтів або організацій несанкціонованим користувачам. У тому ж сценарії витік даних з організації може мати дуже великий вплив на її бізнес у сфері фінансів, довіри та вплив на її бізнес, що стосується фінансів, довіри, втрати клієнтів, а також втрати інтелектуальної власності.

Захоплення облікових записів. Викрадення облікових записів або послуг зазвичай здійснюється за допомогою викрадених облікових даних. Такі атаки включають фішинг, шахрайство та використання вразливостей програмного забезпечення. Зловмисники можуть отримати доступ до критично важливих аспектів хмарних обчислень, таких як конфіденційність, цілісність та доступність послуг.

Внутрішня загроза: Внутрішня загроза - це атака зсередини організації. Це неправомірне використання інформації через зловмисні наміри, нещасні випадки

або шкідливе програмне забезпечення. Співробітники можуть використовувати свій авторизований доступ до хмарних сервісів організації для зловживання або доступу до такої інформації, як рахунки клієнтів, фінансові форми та інша конфіденційна інформація.

Ін'єкції шкідливого програмного забезпечення. Ін'єкції шкідливого програмного забезпечення - це скрипти або код, вбудовані в хмарні сервіси які діють як "дійсні екземпляри" і працюють як SaaS на хмарних серверах. Це означає, що шкідливий код може бути впроваджений в хмарні сервіси і сприйматися як частина програмного забезпечення або сервісу, який працює на самих хмарних серверах.

Мережеві атаки: Мережева атака - це спроба отримати несанкціонований доступ до мережі організації з метою викрадення даних або виконання іншої шкідливої діяльності.

Multi-tenancy: Multi-tenancy або ж Спільна оренда в хмарних обчисленнях виникає, коли кілька споживачів використовують один і той же додаток, що працює в одній операційній системі, на одному і тому ж обладнанні, з однією і тією ж системою зберігання даних, а зловмисник і жертва використовують один і той же сервер.

Зловживання хмарними сервісами: Розширення хмарних сервісів зробило можливим для як малим, так і великим організаціям легко розміщувати величезні обсяги даних. Хакери, спамери та інші злочинці користуються перевагами відповідної реєстрації, простих процедур і порівняно невизначеним доступом до хмарних сервісів для здійснення різноманітних атак, таких як злом ключів або паролів.

Незахищеність API: Інтерфейси прикладного програмування (API) дають користувачам можливість налаштовувати свій досвід роботи в хмарі. API надають програмістам інструменти для створення своїх програм, щоб інтегрувати свої програми з іншим критично важливим для роботи програмним забезпеченням. Вразливість API полягає у комунікації, яка відбувається між додатками. Хоча це

може допомогти програмістам і бізнесу, це також залишає ризики для безпеки, які можна використати.

Недостатня належна перевірка: У сучасних технологіях прогалини в безпеці виникають тоді, коли організація не має чіткого плану щодо своїх цілей, ресурсів та політик для хмарних технологій. Крім того, недостатня належна ретельність може становити загрозу безпеці, коли організація швидко мігрує в хмару, не передбачивши хмару швидко, не передбачивши належним чином, що послуги не будуть відповідати очікуванням клієнтів.

Спільні вразливості: Безпека хмарних сервісів - це спільна відповідальність між провайдером і клієнтом. Таке партнерство між клієнтом і провайдером вимагає від клієнта вживання превентивних дій для захисту своїх даних. Суть полягає в тому, що клієнти та провайдери мають спільні і провайдери мають спільні обов'язки, і якщо ви не виконуєте свої, то ваші дані можуть бути скомпрометовані.

Втрата даних. Дані в хмарних сервісах можуть бути втрачені через зловмисну атаку, стихійне лихо, або знищення даних постачальником послуг. Втрата життєво важливої інформації може бути руйнівною для підприємств, які не мають плану відновлення.

Впровадження шкідливого програмного забезпечення. Ін'єкції шкідливого програмного забезпечення - це скрипти або код, вбудовані в хмарні сервіси які діють як "дійсні екземпляри" і працюють як SaaS на хмарних серверах. Це означає, що шкідливий код може бути впроваджений в хмарні сервіси і розглядатися як частина програмного забезпечення або сервісу, що працює на самих хмарних серверах. Хакери використовують вразливості веб-додатків і вбудовують в нього шкідливий код, змінюючи хід його нормального виконання.

2.2 Вивчення сучасних стандартів захисту даних в хмарних сервісах та їх впливу на забезпечення безпеки інформації

Сучасні стандарти захисту даних в хмарних сервісах мають на меті забезпечити високий рівень безпеки та конфіденційності інформації, що

зберігається та обробляється в хмарному сервісі. Існує дві групи органів стандартів форуму, пов’язані з хмарними обчисленнями. Ті, що входять до складу першої групи, включаючи DMTF, OGF і SNIA, активно працюють сфері мереж та керування розподіленим процесом, а останнім часом додають хмарні обчислення

до своїх завдань. Органи другої групи, включаючи OCC, CSA та GICTF, нещодавно засновані для роботи з хмарними обчисленнями. Найбільш відомі стандарти включають:

ISO/IEC 27001 - ISO/IEC 27001 - це міжнародний стандарт для управління інформаційною безпекою. Він встановлює вимоги до систем управління інформаційною безпекою та визначає процеси, які повинні бути введені в дію для забезпечення безпеки даних в організації.

Ось які рекомендації щодо безпеки хмарних сервісів:

1. Для забезпечення безпеки хмарних середовищ відповідно до вимог ISO/IEC 27001 рекомендується дотримуватися таких принципів:

2. Відповідальність за безпеку даних повинна бути розподілена між хмарним провайдером та користувачем. Хмарний провайдер повинен забезпечити фізичну та логічну безпеку інфраструктури, а користувачі повинні забезпечити безпеку своїх даних, використовуючи доступні інструменти та технології.

3. Для забезпечення конфіденційності та цілісності даних необхідно використовувати ефективні механізми шифрування, які забезпечують захист від несанкціонованого доступу до даних та їх змін.

4. Вимоги до безпеки даних повинні бути визначені на різних рівнях - від рівня доступу користувача до даних до рівня фізичної безпеки дата-центру.

5. Перед використанням хмарного середовища необхідно провести аудиторську перевірку хмарного провайдера на відповідність вимогам безпеки.

6. Хмарний провайдер повинен забезпечити належну організацію управління доступом до даних та інші механізми контролю за доступом до даних.

7. Користувачі повинні бути свідомі можливих ризиків та здійснювати необхідні заходи для захисту своїх даних.

SSAE 16 / ISAE 3402 - стандарти, які встановлюють вимоги до управління ризиками та забезпечення безпеки інформації в хмарних сервісах. Згідно з цими стандартами, провайдери хмарних сервісів повинні забезпечувати високий рівень безпеки даних, а також виконувати регулярні перевірки безпеки.

Ось перелік рекомендацій даного стандарту:

1. Встановлювати відповідні політики безпеки: Важливо мати політики безпеки, які визначають вимоги щодо безпеки даних та інфраструктури. Ці політики повинні бути розроблені з урахуванням SSAE 16 та ISAE 3402.

2. Застосовувати контроль доступу: Потрібно мати контроль доступу до хмарних середовищ, щоб забезпечити, що тільки уповноважені користувачі мають доступ до даних та ресурсів. Контроль доступу можна здійснювати за допомогою аутентифікації та авторизації користувачів, ролей та дозволів.

3. Забезпечувати моніторинг та аудит: Важливо мати механізми моніторингу та аудиту даних та ресурсів в хмарних середовищах. Ці механізми повинні забезпечувати виявлення та реагування на можливі загрози безпеці.

4. Застосовувати шифрування: Шифрування даних є важливим механізмом для захисту від несанкціонованого доступу до даних в хмарних середовищах. Шифрування можна застосовувати для захисту даних під час передачі та зберігання.

5. Використовувати безпечні мережеві з'єднання: Забезпечення безпеки мережевих з'єднань є важливим елементом безпеки хмарних середовищ. Це можна забезпечити за допомогою VPN, мережевих протоколів та інших механізмів захисту мережі..

6. Виконувати процедури з управління ризиками, щоб забезпечити ідентифікацію та оцінку ризиків, а також прийняття відповідних заходів з їх зменшення та контролювання.

7. Забезпечити відповідність середовища безпеці вимогам стандартів.

Варто ще зазначити такі стандати *PCI DSS* і *HIPAA*, які мають схожі рекомендації з вище перерахованих стандартів і їх рекомендаціями.

PCI DSS - стандарт для захисту платіжної інформації, який встановлює вимоги до захисту кредитної інформації та персональних даних в хмарних сервісах.

HIPAA - це стандарт, який має на меті забезпечити конфіденційність та безпеку медичних даних у хмарних сервісах.

2.3 Функції та особливості використання Cisco Stealthwatch Cloud

Cisco Stealthwatch Cloud — це рішення для моніторингу мережевої безпеки в хмарних середовищах, яке забезпечує підтримку різноманітних платформ, таких як AWS, Azure, Google Cloud та інших. Він забезпечує збір, аналіз та візуалізацію даних про мережевий трафік, щоб допомогти організаціям виявляти загрози та забезпечувати безпеку мережі. Такі функції там пропонує виробник:

Моніторинг трафіку. Stealthwatch Cloud здатен збирати дані про трафік у реальному часі, що дозволяє оперативно виявляти та реагувати на загрози та інциденти безпеки, це його найголовніша задача та перевага на Світовому ринку.

Машинне навчання та аналіз поведінки: Cisco Stealthwatch Cloud використовує машинне навчання для аналізу поведінки мережевих пристроїв та даних передачі, що дозволяє виявляти відхилення від звичайних шаблонів та ідентифікувати потенційні загрози безпеки. Крім того, система має можливість аналізувати мережевий трафік та відслідковувати аномальну активність користувачів, що дозволяє ефективно виявляти та усувати потенційні загрози для мережі.

Виявлення загроз. Рішення використовує машинне навчання та аналіз поведінки, щоб виявляти загрози, такі як кібератаки, атаки вірусів та шкідливі програми.

Система сповіщень. Stealthwatch Cloud може надсилати сповіщення про потенційні загрози безпеки на мобільний телефон або електронну пошту, що дозволяє оперативно реагувати на інциденти безпеки.

Перевірка внутрішньої безпеки: Cisco Stealthwatch Cloud допомагає виявляти потенційні вразливості та слабкі місця в мережі, щоб організації могли підвищити рівень безпеки мережі.

Візуалізація даних. Рішення надає візуальну карту мережі, що дозволяє легко відслідковувати трафік між різними компонентами мережі та виявляти аномалії. Як доповнення надає детальну інформацію про мережевий трафік, що дозволяє швидко виявляти загрози та реагувати на них.

Інтеграція продкту та сумісність з іншими рішеннями. Cisco Stealthwatch Cloud легко інтегрований з іншими системами безпеки, що дозволяє організаціям швидко виявляти та реагувати на загрози, також інтегрується з іншими рішеннями Cisco, такими як Cisco Identity Services Engine (ISE), що дозволяє забезпечувати комплексний захист мережі.

Підтримка мультихмарних середовищ Stealthwatch Cloud може працювати в різних хмарних середовищах, включаючи AWS, Azure та Google Cloud, що дозволяє забезпечувати захист мережевої безпеки в будь-якому хмарному середовищі. Також надає широкий спектр підтримки та підтримується 24/7.

2.4 Алгоритм роботи з Cisco Stealthwatch Cloud

Cisco Stealthwatch Cloud збирає дані про мережеву активність з різних джерел, таких як мережеві пристрої, файрволи, системи безпеки, хост-комп'ютери тощо. Дані можуть включати інформацію про трафік мережі, кількість пакетів, час відправлення та отримання пакетів, IP-адреси та іншу інформацію.

Cisco Stealthwatch Cloud обробляє та агрегує дані з різних джерел, щоб створити цілісний образ мережевої активності. Саме агрегація даних відбувається в процесі збору телеметричних даних з різних джерел, таких як NetFlow, syslog, та інших.

Дані збираються в одній точці і обробляються за допомогою алгоритмів машинного навчання, для більш точного аналізу мережевої активності, щоб виявити аномальну поведінку в мережі та інші загрози безпеки. Когнітивна

аналітика може вчитися на тому, що бачить, і адаптуватися до зміни поведінки мережі з часом. Телеметрія мережі збирається за допомогою мережеваї телеметрії, яка збирається за допомогою Flow Collector і надсилається до Cognitive Analytics для подальшого аналізу. Stealthwatch з Cognitive Analytics покращує видимість потоків трафіку, централізуючи управління мережевим і веб-трафіком в консолі управління.

Замість того, щоб розшифровувати трафік, Stealthwatch з Cognitive Analytics визначає зловмисні шаблони в зашифрованому трафіку, щоб виявити загрози і прискорити відповідної реакції.

Cisco Stealthwatch Cloud застосовує різноманітні аналітичні техніки та алгоритми, щоб виявити потенційні загрози безпеці мережі, такі як атаки зломників, незаконний доступ до мережі, шкідливе програмне забезпечення та інші. Це включає в себе аналіз мережевих потоків, зібраних з використанням технологій NetFlow, IPFIX та других, а також аналіз системних журналів, даних аутентифікації та авторизації, даних з безпекових пристроїв та інші.

Після збору даних вони проходять через ряд аналітичних модулів, що використовуються для виявлення потенційно шкідливих дій та загроз. Аналіз даних в Stealthwatch Cloud також може включати в себе використання машинного навчання та штучного інтелекту для виявлення аномальних дій та поведінки в мережі.

На основі аналізу даних Cisco Stealthwatch Cloud визначає рівень ризику для кожної виявленої загрози. Твкож варто зазначити, що на основі аналізу трафіку та даних про використання ресурсів мережі, Stealthwatch Cloud надає рекомендації щодо поліпшення безпеки мережі. Це дозволяє адміністраторам мережі швидко виявляти та вирішувати потенційні проблеми безпеки мережі.

Cisco Stealthwatch Cloud надає привілейним адміністраторам мережі можливість встановлювати різні заходи безпеки, такі як блокування певних IP-адрес або відключення певних мережевих портів, для зменшення ризику для мережі.

2.5 Дослідження застосування Cisco Stealthwatch Cloud для захисту хмарних сервісів

Сучасні мережеві середовища мають новий тип загроз, які не обов'язково які не обов'язково можуть бути помічені брандмауерами на кордоні мережі. Коли мережі збільшуються в масштабах і багато хостів надсилають трафік в мережу, користувачеві стає важче зрозуміти, що насправді відбувається в мережі.

Stealthwatch збирає телеметричні дані з кожної частини мережі і застосовує до них передову аналітику безпеки. Він створює базову лінію звичайної веб-активності та мережевої активності для мережевого хоста і застосовує контекстно-орієнтований аналіз для автоматичного для автоматичного виявлення аномальної поведінки. Stealthwatch може ідентифікувати широкий спектр атак, включаючи шкідливе програмне забезпечення, атаки нульового дня, розподілені спроби відмови в обслуговуванні (DDoS), сучасні постійні загрози (APT) та внутрішні загрози.

Система Stealthwatch може бути налаштована, але її обов'язковими основними компонентами є ліцензія на вимірювання витрати, Flow Collector та консоль керування. Ліцензія Flow Rate необхідна для збору, управління та аналізу телеметрії потоку та агрегованих потоків у консолі керування. Ліцензія на швидкість потоку також визначає обсяг потоків, які можна збирати, і ліцензується на основі потоків в секунду. Довжина пакетів, час прибуття та тривалість як правило, відрізняються для шкідливого програмного забезпечення ніж для безпечного трафіку. На рис.2.1 графічно зображено як виявляють аномалії, тобто зловмисного зашифрованого трафіку.

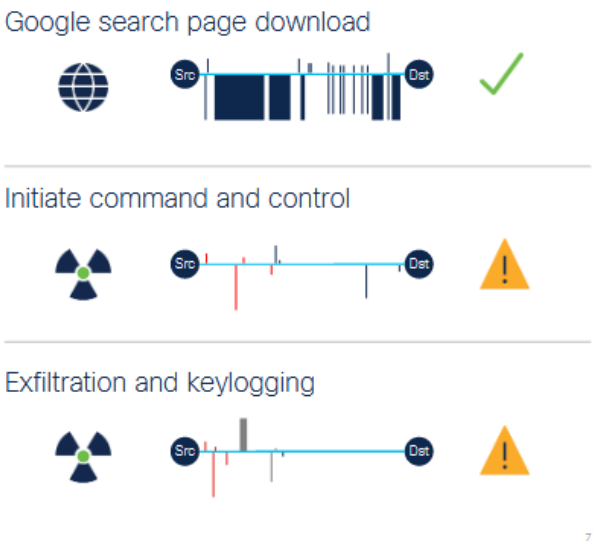

Рис.2.1. Виявлення зловмисного зашифрованого трафіку

Ліцензія Stealthwatch Endpoint License — це додаткова ліцензія, яка забезпечує більш ефективні, контекстно-орієнтовані розслідування пристроїв кінцевих користувачів, які демонструють підозрілу поведінку. Ліцензія дозволяє експортувати дані кінцевих точок.

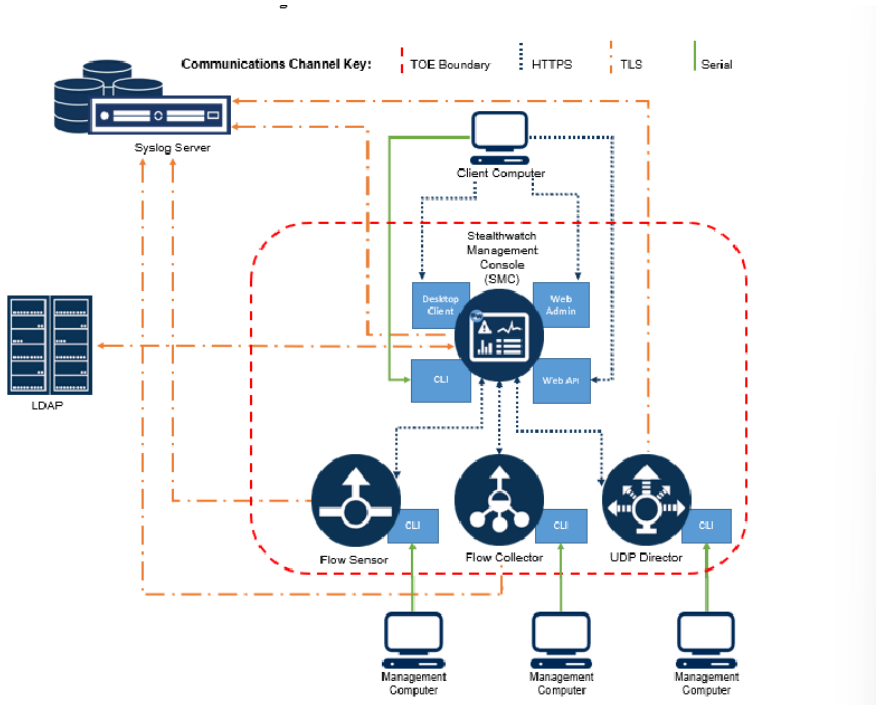

Рис.2.2. Демонстраційна схема протоколів та з’єднань

Дана схема показує протоколи та з'єднання (TLS, HTTPS та послідовні з'єднання), які мають відношення до вимог NDcPP. NDcPP — "Найвищі вимоги

захисту критичних об'єктів інформації для безпечних продуктів". Це є стандартом, розробленим Міжнародним інститутом стандартів і технологій США (NIAP), який визначає вимоги до безпеки для продуктів та систем, що містять критичну інформацію. Компоненти TOE (Target of Evaluation) також використовують інші протоколи (наприклад DNS, NetFlow і sFlow. Кожен пристрій містить DNS-клієнт для визначення FQDN (наприклад, для LDAP-серверів, центрів сертифікації, точок розподілу URL-адрес), серверів LDAP, центрів сертифікації, точок розподілу URL-адрес і OCSP-відповідачів). FC отримує трафік NetFlow або sFlow (залежно від того, чи було встановлено технологію передачі даних в масштабованих обчислювальних системах та зберігання даних. FC у режимі sFlow або NetFlow) від UDPD та FS. FS відстежує мережевий трафік (через свій проміжний (пасивний) інтерфейс) і генерує дані sFlow або NetFlow для передачі на FC. UDPD отримує sFlow або NetFlow від відстежуваних пристроїв і перенаправляє цей трафік на FC.

Категорія тривоги — це місце, до якого певний перелік подій безпеки додає бали індексу бали. Коли мережева активність відповідає або перевищує певний набір критеріїв, визначених для цієї категорії тривоги категорії тривоги, це спричиняє тривогу. Кожна категорія тривог має власний перелік подій безпеки, які додають до неї індексні бали і можуть спричинити генерування тривог. Подія безпеки - це алгоритм який шукає певну поведінку і може сповіщати про неї у мережі, залежно від налаштувань, застосованих у політиках. Нижче наведено докладнішу інформацію про категорії тривог інформаційної панелі(2.3).

Рис.2.3. Аналітична панель мережевої безпеки

Індекс занепокоєння та цільовий індекс. Відстежує хости, індекс занепокоєння яких або перевищив поріг індексу занепокоєння (CI), або стрімко збільшився. Якщо подія викликана хостом-джерелом, вона призводить до тривоги за індексом занепокоєння. Якщо подія спричинена цільовим хостом, вона призводить до тривоги за цільовим індексом.

Розвідка. Вказує на наявність несанкціонованих і потенційно зловмисних сканувань за допомогою TCP або UDP і на хостах організації.

Командування та контроль Вказує на наявність заражених ботами серверів або хостів у вашій мережі, які намагаються зв'язатися з C&C-сервером.

Експлуатація. Відстежує прямі спроби хостів скомпрометувати один одного, наприклад, за допомогою розповсюдження черв'яків та перебору паролів грубою силою.

Джерело DDoS-атаки. Вказує на те, що хост був ідентифікований як джерело DDoS-атаки.

DDoS-ціль. Вказує на те, що хост було визначено як ціль DDoS-атаки.

Накопичення даних. Вказує на те, що хост-джерело або хост-ціль у мережі завантажив незвичний обсяг даних з одного або декількох хостів.

Ексфільтрація. Відстежує внутрішні та зовнішні хости, на які було передано аномальний обсяг даних. Якщо хост викликає кількість таких подій, що перевищує налаштований поріг, це призводить до тривоги про витік даних.

Витік даних. Порушення політики встановленою організацією. Об'єкт демонструє поведінку, яка порушує звичайні мережеві політики.

Аномалія. Відстежує події, які вказують на те, що хости поводяться ненормально або генерують трафік, який є незвичний, але не узгоджується з іншою категорією активності.

Основні компоненти інструментів Stealthwatch, такі як датчик потоку, колектор потоку і консоль управління Stealthwatch (SMC) з'єднані для належної видимості всього середовища/мережі для аналізу трафіку і потоків. інструмент Stealthwatch може виявити будь-яку аномалію в мережі, яка відхилилася від базової лінії, спостерігаючи за рівнем потоків, який генерує сповіщення, якщо щось

трапляється. Крім того, інформаційна панель, щосекунди відображає поточну поведінку в мережі і надсилає сповіщення адміністратору, якщо щось відхиляється від базової лінії, для негайного реагування. Це досягається за допомогою сповіщень, які генерує SMC на основі базової лінії аналітики конфігурацій і надсилає сповіщення адміністратору в разі виникнення будь-якої проблеми для негайного реагування.

Висновки до другого розділу

Проаналізовано, функції та особливості використання Cisco Stealthwatch Cloud, здебільше його перваги під час використання.

Досліджено, мету та алгоритм роботи Cisco Stealthwatch Cloud, його корисність та сертифікацію про захисту інформації хмарних середовищ.

Зазначено та обґрунтовано, що система Cisco Stealthwatch Cloud, як і будь яка інша має бути правильно налаштована, задля зменшення ризиків витоку даних та втрати коштовної інформації.

3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ ІЗ ВИКОРИСТАННЯМ STEALTHWATCH CLOUD

3.1 Налаштування моніторингу приватної мережі Stealthwatch Cloud

Підключення датчика до порталу Stealthwatch Cloud

Для початку необхідно налаштувати хмарного датчика моніторингу приватної мережі Stealthwatch Sensor для отримання телеметрії NetFlow з мережевого середовища. Для того щоб скористатися порталом Stealthwatch Cloud, щоб переглянути детальну інформацію про спостережуваний трафік, таким чином продемонструється, які сповіщення доступні в Stealthwatch Cloud, оскільки він виконує базове налаштування середовища.

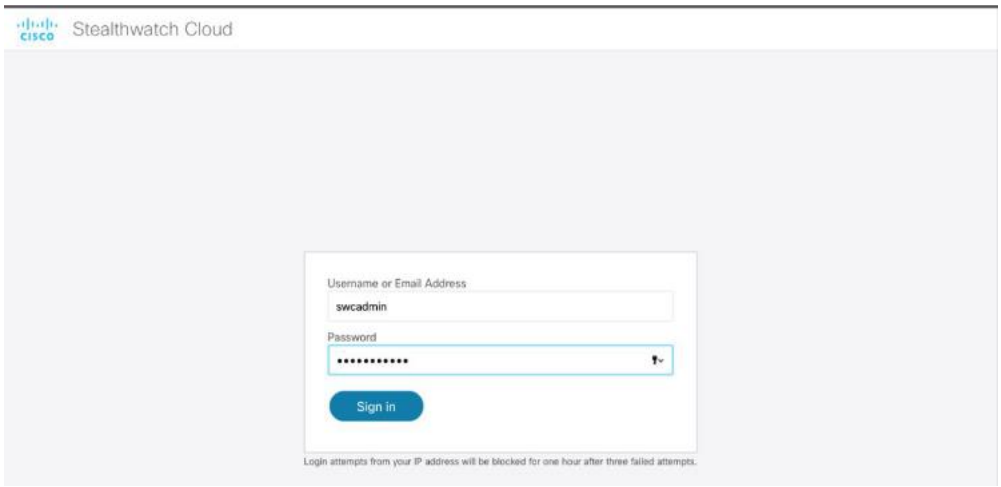

Рис.3.1. Вхід

Необхідно для початку виконати вхід у сиситему, вводячи пароль, оскільки було сказано неоднаразово, що Система Stealthwatch може бути налаштована, але її обов'язковими основними компонентами є ліцензія.

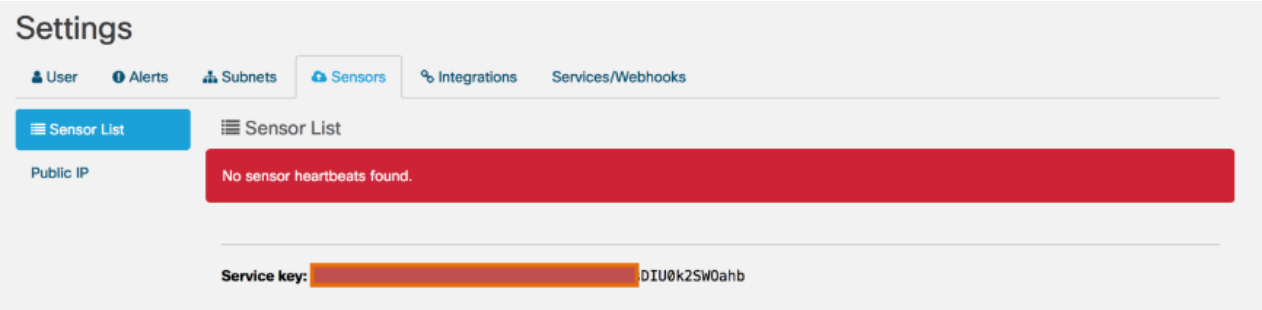

Рис.3.2. Копіювання сервісного ключа

Реагуваня конфігураційний файл config.local датчика, щоб змінити назву датчика так, як вона буде відображатися на порталі і ручне додавання сервісного ключа порталу, щоб зв'язати датчик з порталом. Для цього необхідно прейти до кінця списку датчиків і скопіювати сервісний ключ.

Додавання ключа служби вручну зазвичай не потрібне в польових умовах, якщо не маєте справу зі специфічними сценаріями розгортання зі специфічними сценаріями розгортання. Наприклад, якщо кілька датчиків розміщено в центральному місці, наприклад, на MSSP, і вони призначені для різних порталів. У цьому випадку, якщо загальнодоступна IP-адреса використовується для кількох датчиків, датчик може бути некоректно приєднаний до неправильного порталу.

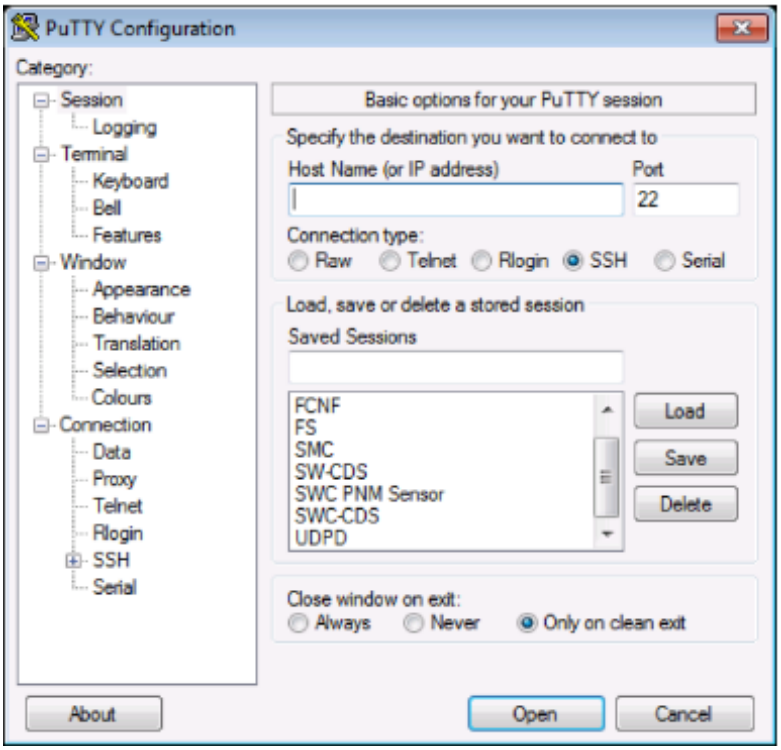

Рис.3.3.Зміна конфігурації датчика

Щоб змінити конфігурацію датчика треба ввести вручну зміни до конфігурації датчика, у командному рядку : sudo nano /opt/obsrvbl-ona/config.local , далі у файлі config.local наступний запис:

OBSRVBL_ONA_NAME=SENSORNAME, та замінити значення, вказане в полі SENSORNAME, на ім'я для ідентифікації датчика на порталі Stealthwatch Cloud. Додвши наступний рядок та замінивши <service-key> на сервісний ключ порталу: OBSRVBL_SERVICE_KEY="<service-key>"

Рис.3.4. Демонстрація вводу в командний рядок для перезапуску служби

У командному рядку потрібно ввести sudo service obsrvbl-ona restart ,щоб перезапустити службу Stealthwatch Cloud. Це також перезапустить інші налаштовані служби.

Далі для визначення публічних IP-адрес датчика та додавання його до Stealthwatch Stealthwatch Cloud Portal потрібно відкрити та ввести у командному рядку:

curl https://sensor.ext.obsrvbl.com

Значення помилки "невідома ідентичність" означає, що датчик не пов'язаний з порталом. Скопіювавши IP-адресу, яка вказана для значення "ідентифікатор"і буде публічною IP-адресою для датчика SWC PNM облікового запису.

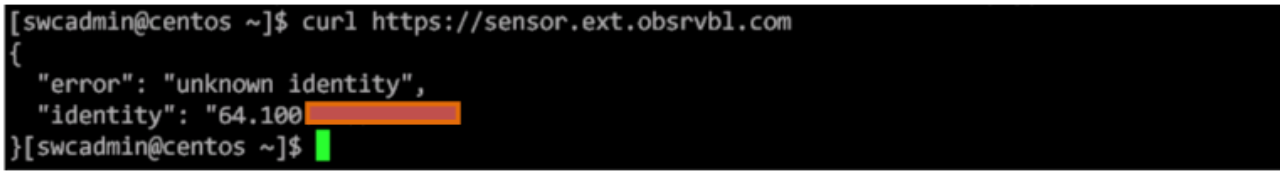

Рис.3.5. Демонстрація вводу в командний рядок IP-адресу

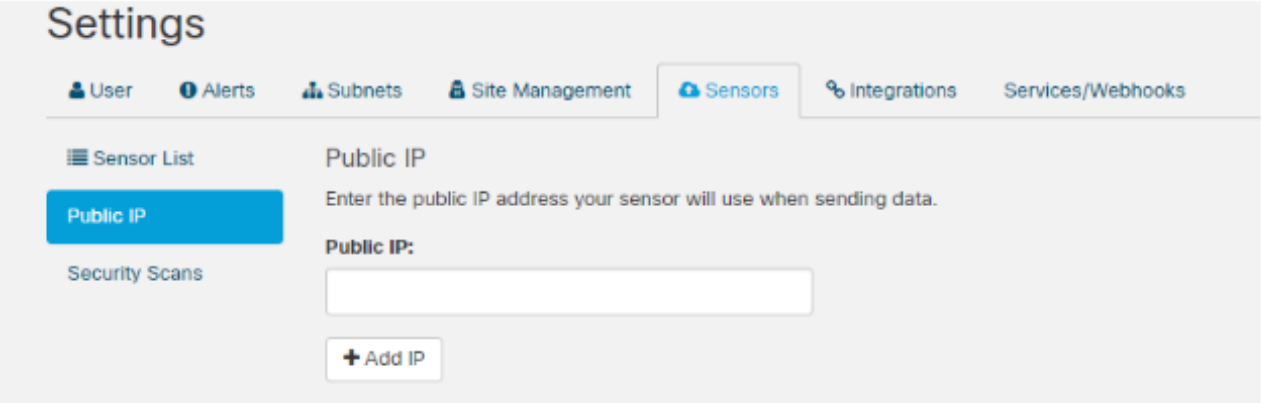

Рис.3.6. Налаштування публічної IP-адреси

Вказавши Stealthwatch Cloud приймати повідомлення від датчиків з потрібної публічної IP-адреси та ввівши "ідентифікаційну" IP-адресу у полі *Публічна IP-адреса*.

Якщо датчик відображається і показує активне серцебиття, а також те, що він отримує дані, це означає, про успішне додання його до порталу облікового запису.

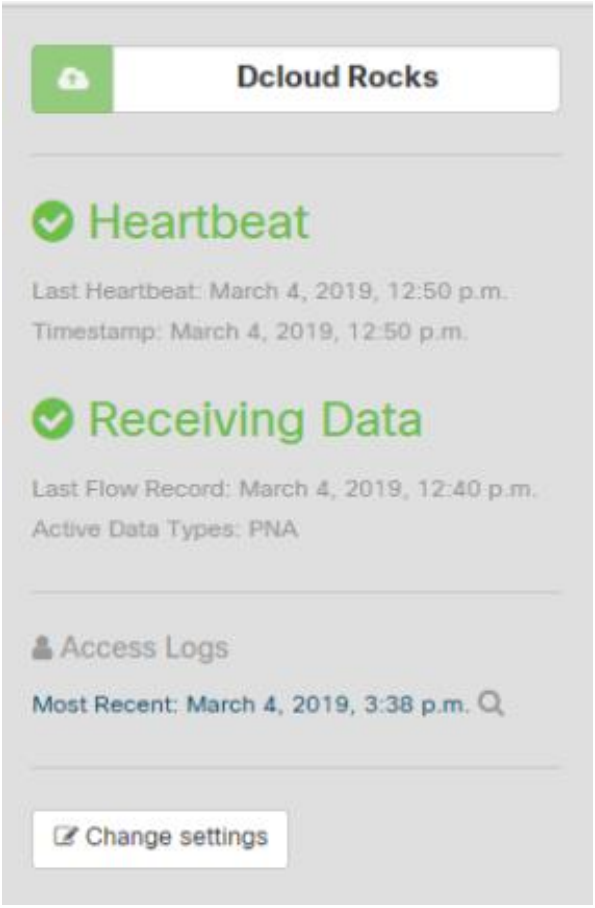

Рис. 3.7. Серцебиття

3.2 Налаштування збору телеметрії Netflow у Cisco Stealthwatch Cloud

NetFlow є протоколом моніторингу мережі, який використовується для збору та аналізу мережевих даних. В Cisco Stealthwatch Cloud, налаштування NetFlow дозволяє отримувати дані про трафік, що проходить через мережу, і забезпечує можливість аналізу цих даних для виявлення загроз безпеці.

Щоб визначити параметри збору, треба обрати вкладку Netflow/IPFIX та натиснути "Додати новий зонд. Також ввести такі налаштування потоку та зберегти по завершенню:

- NetFlow v9, на порт 2055/udp
- IPFIX, на порт 4739/udp

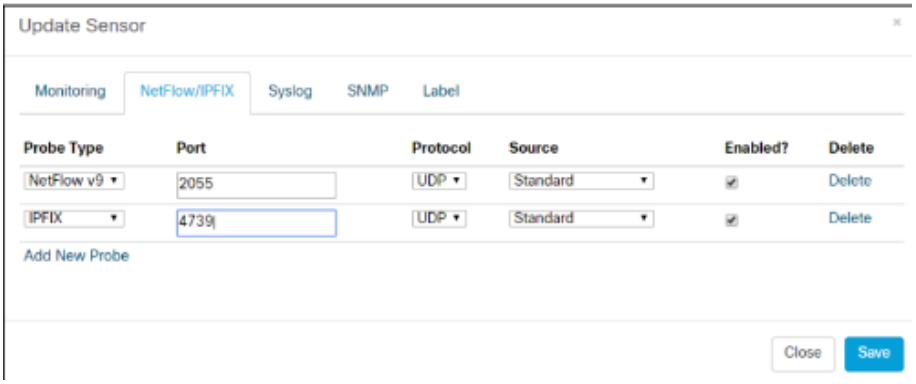

Рис. 3.8. Демонстрація налаштуваня збору телеметрії

Якщо "Активні типи даних" будуть містити PNA + IPFIX, коли потоки почнуть збиратися, то це означає про успішне налаштувння розгорнутого хмарного датчика Stealthwatch на прийом NetFlow v9 та IPFIX телеметрії на портах 2055 і 4739 відповідно(3.9).

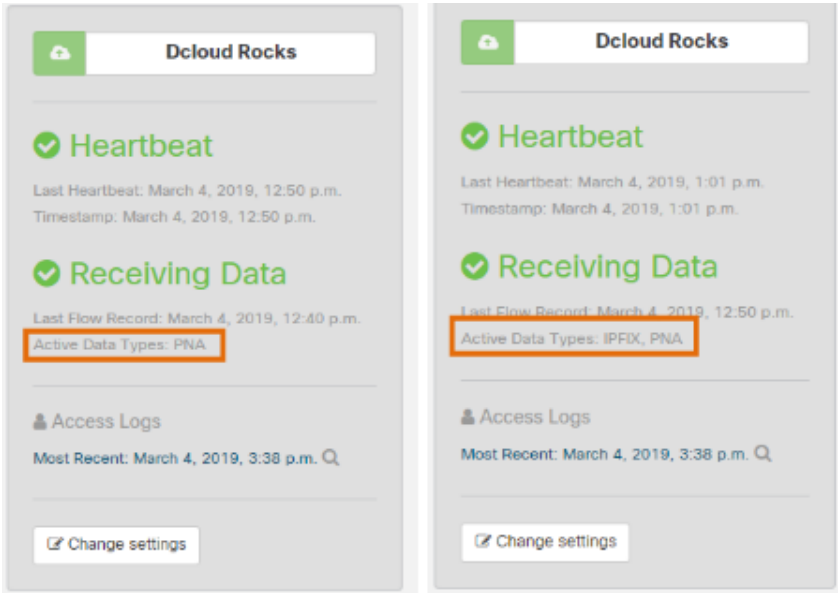

Рис. 3.9. Активні типи даних

3.3 Перевірка запущеної конфігурації, збору мережевого потоку та датчика

Тут продемонстровано, як перевірити, що конфігурація, визначена на хмарному порталі та була успішно застосована до датчика PNM. Також, як перевірити, що різні хмарні сервіси Stealthwatch Cloud працюють на сенсорі PNM Senor, та пов'язані з хмарним порталом Stealthwatch Cloud, з командного рядка датчика, а також відповідно, перевірка що Netflow досягає датчика.

Для початку потрібно у командному рядку ввести:

sudo nano /opt/obsrvbl-ona/config.auto та переконатися, що зміни, внесені через портал, відобразилися в конфігураційному файлі.

Рис. 3.10.Пергляд змін

Перевірка вхідного телеметричного трафіку NetFlow

Для того щоб перевірити наявність вхідної телеметрії NetFlow v9 на порту, який було вказано під час налаштування конфігурації, в командному рядку було введено sudo tcpdump -i eth0 -n -c 100 "port 2055"

Якщо телеметрія NetFlow успішно приймається —повинні побачити результати.

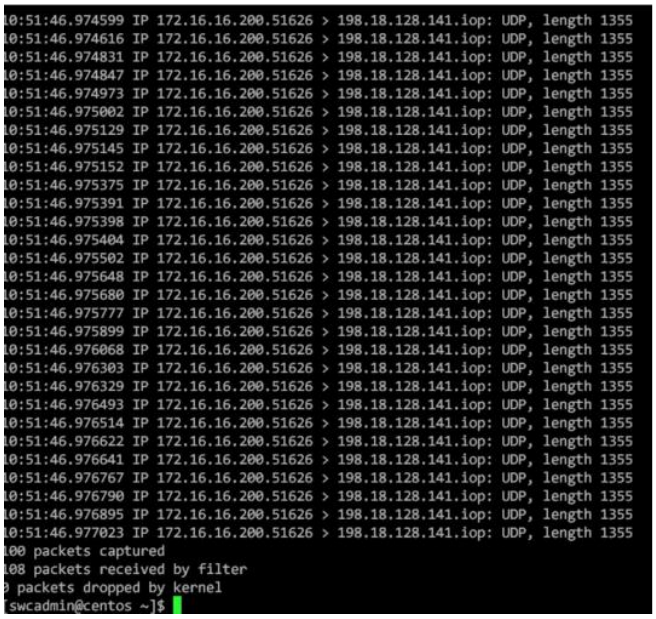

Рис. 3.11. Демонстрція результатів

Далі повторюючи процес для телеметрії IPFIX, знову ввівши команду і змінивши номер порту з 2055 на 4739.

Трафік IPFIX у цьому середовищі розріджений. Для цілей цього тесту, якщо не бачити результатів для IPFIX не з'являються вчасно, треба переконатися, що вводили в терміналі команду tcpdump для прослуховування трафіку на порту 4739 і запускали скрипт генерації трафіку з меню "Пуск" Windows (Start SWC Traffic). Start SWC Traffic), щоб змусити трафік з'явитися

Перевірка запущених служб

Було перевірено, що різні основні служби, пов'язані з Stealthwatch Cloud, запущені з датчика командного рядка датчика. Це основні сервіси Stealthwatch, пов'язані з хмарою, які можуть бути запущені на пристрої Sensor.

Service	Enabled by default?	Description
obsrvbl-ona	Yes	Monitors for configuration changes and handles automatic updates. Starting this service also starts the other configured services.
log-watcher	Yes	Tracks the sensor's authentication logs.
pdns-capturer	Yes	Collects passive DNS queries.
pna-monitor	Yes	Collects IP traffic metadata.
pna-pusher	yes	Sends IP traffic metadata to the cloud.
hostname-resolver	yes	Resolves active IP addresses to local hostnames.
flowcap	no	Listens for NetFlow data sent by routers and switches.
ipfix-pusher	no	Sends NetFlow data to the cloud.
notification-publisher	no	Relays observations and alerts over syslog or SNMP.

Рис. 3.12. Сервіси flowcap і ipfix_pusher та можливості споживання NetFlow

Якщо в результатах сервіси flowcap і ipfix_pusher, це означає, що можливості NetFlow споживання можливості споживання NetFlow працюють.

3.4 Використання хмарного порталу Stealthwatch

Тепер необхідно використати портал для перегляду телеметрії, зібраної з розгорнутого та налаштованого датчика. Для цього потрібно залишити значення за

замовчуванням поточного дня. Як можна побачити, показано зібраний мережевий трафік. Можна натиснути на інші вкладки, щоб змінити дані та візуалізації, що відображаються для даних у вказаному діапазоні.

На головній інформаційній панелі необхідно перейти до вкладки *Моделі* > *Трафік сеансів*. Та Залишити значення за замовчуванням поточного дня натиснувши *Оновити*.

Рис. 3.13.Інформаційна панель *Трафік сеансів*

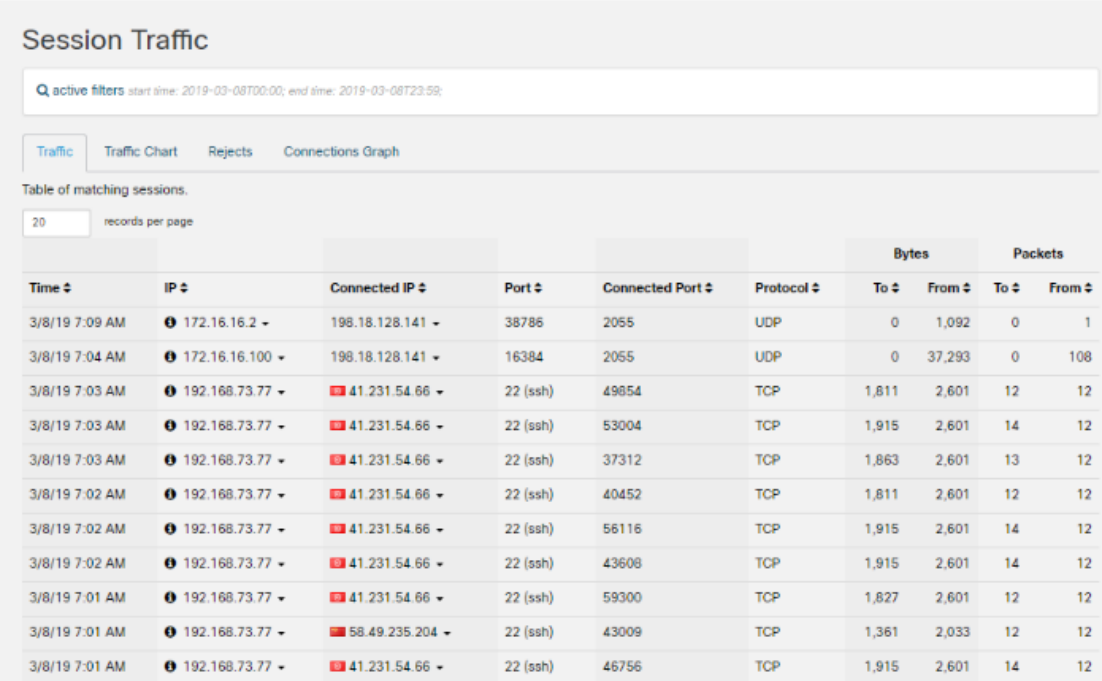

Рис. 3.14.Демонстація використання хмарного порталу Stealthwatch

Далі повинно бути створенно правило Blacklist трафіку. Визначене правило чорного списку буде сповіщати, коли дві IP-адреси, які не повинні взаємодіяти, будуть обмінюються даними.

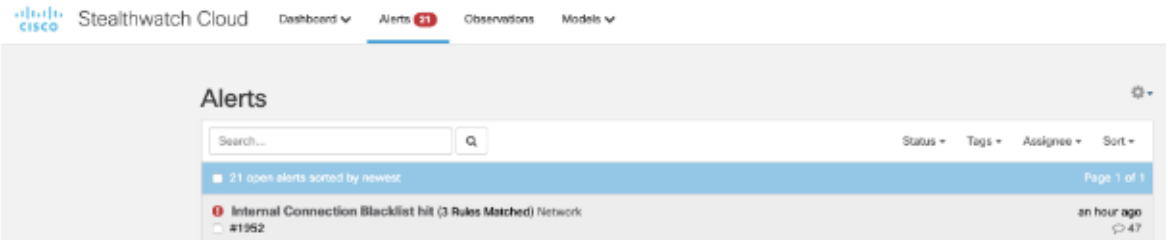

Рис. 3.15. Правило Blacklist

Для завершення налаштування потрібно переглянути кінцеві точки в диспетчері пристроїв. Для цього необхідно виконати вхід на портал, перейти до меню пошуку та ввести IP-адресу 10.201.3.142.

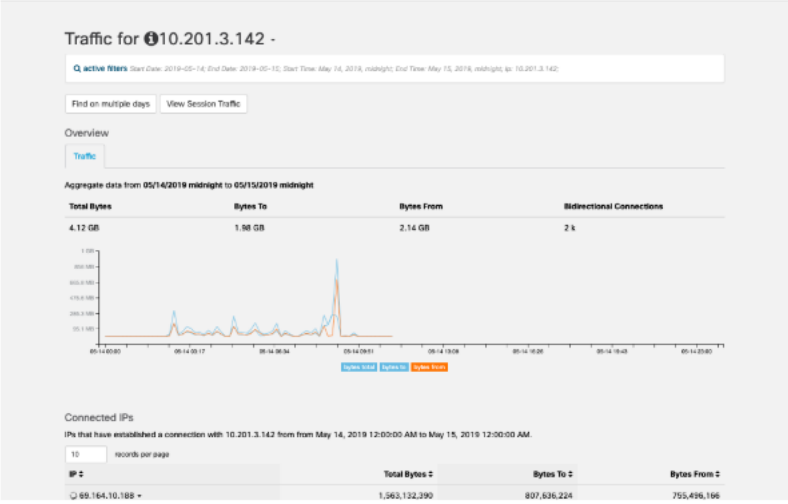

Рис. 3.16. Перегляд кінцевих точок

Зазначаємо зведення трафіку для цієї кінцевої точки, включаючи дані про IP-адреси, до яких вона підключилася та найпопулярніші порти, що використовуються. Бачимо екран огляду кінцевої точки, на якому буде показано всю зібрану інформацію про хост. Якщо датчик було додано нещодавно, дані можуть бути обмеженими, це може зайняти до 30 хвилин.

Рис. 3.17. Екран огляду всієї інформації кінцевої точки

Висновки до третього розділу

Досліджено та продемонстровано налаштування моніторингу приватної мережі Stealthwatch Cloud, що є головним аспектом захисту інформації хмарних середовищ і найчастішою ланкою для кіберзлочинців.

Проаналізовано, використання хмарного порталу Stealthwatch налаштування збору телеметрії Netflow у Cisco Stealthwatch Cloud, його ефективність та роботу.

Розроблено та обґрунтовано рекомендації щодо впровадження та налаштування рішення задля покращення захисту інформації хмарних середовищ.

ВИСНОВКИ

У роботі отримано наступні теоретичні та практичні результати:

1) Проаналізовано, популярність, можливості хмарних сервісів та безпосередньо їх вразливості.

2) Досліджено, різні методи захисту хмарних сервісів та їх використання для забезпечення безпеки в хмарних середовищах.

3) Також розглянуті сучані стандарти щодо захисту хмарних середовищ та їх рекомендації щодо їх захисту.

4) Зазначено основні функції та вимоги до рішень для моніторингу мережі хмарних сервісів з використанням Cisco Stealthwatch Cloud. Та розглянуто методи налаштування заходів безпеки з використанням Cisco Stealthwatch Cloud.

5) Розроблені рекомендіції щодо покращення безпеки вже існуючих методів.

6) Зроблено висновок, що людський фактор все ще лишається найбільшою загрозою для інформаційної безпеки у хмарних середовищах. Некомпетентність працівників — ось на чому мають акцентувати компанії. Тож потрібно моніторити загрози, які можуть виникнути, дотримуватись впроваджених компаніями політик безпеки.