ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ РІШЕННЯ CISCO CLOUDLOCK»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Місевіч К. С.
(прізвище та ініціали)

Керівник Гахов С.О.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

ВСТУП

Актуальність дослідження. Актуальність дослідження сучасних технологій забезпечення безпеки в хмарному середовищі зумовлено їх розповсюдженням у корпоративному сегменті. Сьогодні у споживачів виникає низка питань щодо проблем безпеки та конфіденційності даних. Окрім вже відомих ризиків безпеки, що виникають в обчислювальних системах, з'єднаних з Інтернетом, хмарні системи мають своєрідні проблеми безпеки та конфіденційності по причині віртуалізації хмар та їх багаторівневої структури.

Захист хмарного середовища є обов'язковою складовою забезпечення кіберзахисту у корпоративному сегменті. На сьогоднішній день класичні методи до захисту даних у хмарному середовищі вже не забезпечують належний рівень захисту від сучасних кіберзагроз.

Інтеграція системи контролю та безпеки даних у хмарному середовищі дозволяє проводити моніторинг подій та вчасно ліквідувати загрози безпеки всередині та поза межами хмарного середовища. Крім несанкціонованого витоку конфіденційної інформації існують інші види інформаційних загроз, які націлені на часткове або повне зупинення робочих процесів в компанії, блокування оперативного доступу до належних зовнішніх та внутрішніх інформаційних ресурсів, погіршення продуктивності хмарної інфраструктури або її повне зупинення тощо.

Відомо, що сучасна IT-сфера відрізняється швидким темпом розвитку та великою кількістю інноваційних рішень. Через специфічне функціонування хмарних сервісів, класичні нормативно-правові методи, практики та механізми стають найчастіше неефективними. Для забезпечення ефективного захисту конфіденційних даних використовуються сучасні методи та рішення, що забезпечують комплексний підхід до питання захисту даних у корпоративному сегменті.

У сучасних розробках рішення подібних задач мають певні недоліки:

відсутність уніфікованого підходу для забезпечення стійкості функціоналу хмарних ресурсів через динаміку змін функцій віртуальних машин в хмарному середовищі; використання незахищених інтерфейсів додатків.

Комплексний підхід до захисту даних в хмарному середовищі побудований на конфіденційності, цілісності та доступності. Саме тому компанія Cisco створила брокер безпеки доступу до хмарного середовища (CASB, Cloud Access Security Broker), що забезпечує кібернетичну безпеку в хмарній системі на найвищому рівні. Саме тому, для дослідження була обрана технологія на базі рішення саме цієї компанії.

Отже, доведена актуальність теми даної магістерської роботи, основний зміст якої полягає у дослідженні технології захисту хмарного середовища на базі рішення Cisco Cloudlock.

Об'єкт дослідження – процес забезпечення кібербезпеки хмарного середовища.

Предмет дослідження – методи та засоби забезпечення кібербезпеки хмарного середовища на базі Cisco Cloudlock.

Мета роботи – розробити варіант технології забезпечення кібербезпеки хмарного середовища та рекомендації щодо застосування технології захисту хмарного середовища в корпоративному сегменті.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту хмарного середовища;

встановити сутність завдань захисту хмарного середовища;

проаналізувати існуючі технології захисту хмарного середовища;

проаналізувати методи та засоби забезпечення захисту хмарного середовища;

проаналізувати основні функції та принципи реалізації захисту хмарного середовища.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання захисту даних у хмарному середовищі.

Практичне значення одержаних результатів полягає у тому, що запропонована технологія захисту хмарного середовища на базі рішення Cisco Cloudlock може бути використана у корпоративному сегменті для оптимізації

робочих процесів за умови збереження конфіденційності, доступності та цілісності даних у хмарному середовищі.

Апробація:

1. Колісник Д. Р., Місевич К. С., Коваленко С. В. Системна архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки: огляд туманних обчислень, впровадження аудиту інтернету речей // [Електронний ресурс]. – Науковий журнал «Сучасний захист інформації». – Київ, ДУТ. – с. 34-38 Режим доступу : World Wide Web. – URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2442.

2. Місевіч К.С. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення CISCO CLOUDLOCK // [Електронний ресурс]. – Збірник матеріалів XIII НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ. – Київ, ВІТІ, - с. 195 Режим доступу : World Wide Web. – URL: http://www.viti.edu.ua/files/zbk/2020/c_2020.pdf .

1 АНАЛІЗ ПРОБЛЕМИ ХМАРНИХ ТЕХНОЛОГІЙ ТА СЕРВІСІВ

1.1. Визначення та характеристика хмарного середовища

Концепція хмарних обчислень з'явилася, коли американський вчений Джон Маккарті висловив припущення, що у майбутньому комп'ютерні обчислення стануть надаватися подібно комунальним послугам.

Популяризація мереж з високою потужністю, низька собівартість комп'ютерів і пристроїв для зберігання даних, а також активне впровадження віртуалізації призвели до зростання та розвитку хмарних технологій. Сьогодні користувачі можуть не перейматися роботою обладнання технологічної інфраструктури «в хмарі», яка підтримує їх роботу.

Хмари - це великий ресурс простих у використанні та доступних віртуалізованих сервісів (наприклад апаратні засоби, платформи розробки, послуги та інше). Ці ресурси зазвичай динамічно реконфігуровані, для того, щоб пристосуватися до нестабільного навантаження, що також дозволяє ефективно використовувати ресурси.

Подібні ресурси як правило, експлуатується за моделлю оплати за фактичне використання, в якій є гарантії, що запропоновані провайдером певної інфраструктури, що включають індивідуальні угоди про рівень послуг (SLA). Пошук визначення може бути альтернативним підходом для кращого розуміння базових елементів хмарних технологій з технічної сторони.

Наприклад, одне з визначень сприймає хмарну модель як певне рівняння, що описує зв’язок між базовими компонентами хмари. Це можуть бути як центри обробки даних, так і апаратне обладнання, що застосовуються для створення хмари. Визначення хмарних обчислень має втілювати основні характеристики, що являють собою цінність хмар. NIST визначив більшу частину характеристик, які активно застосовуються.

Можливість самообслуговування. Хмарні обчислювальні ресурси надаються за необхідністю користувача та по певном плану, не вимагаючи особистої взаємодії

з провайдером послуг. Це забезпечує економію часу, економічність та зручність використання.

Відкритий доступ по мережі. Послуги хмари головним чином доступні через мережу Інтернет, що включає стандартні механізми та протоколи для підтримки пристроїв і різних типів платформ.

Поєднання ресурсів. Хмарні ресурси на фізичному рівні базуються на технології віртуалізації та розподіляються серед користувачів залежно від потреб споживання. Фізичні обмеження ресурсів віртуально забезпечуються та вилучаються автоматизовано ха необхідністю.

Послуги розрахунку. Послуга надається відповідно до бізнес-моделі «оплата за використання», тобто користування послугами та ресурсами можливо виміряти та розраховувати вартість за певний, окремо взятий сеанс користувача.

Швидкість. В режимі реального часу забезпечення та вилучення хмарних послуг здійснюється дуже швидко, динамічно та відповідно попиту.

Незалежність від місцевості. Хмарні ресурси не залежать від географічній локації, при умові можливості доступу зв’язку. Користувачі хмар також можуть мати доступ до послуги, де б вони не знаходились за тими самими умовами.

Хмарні обчислення являють собою кардинальну зміну парадигми в розгортанні обчислювальних систем. Хмарні обчислення - це про нескінченно масштабовану, загальнодоступну систему обчислень, що має можливість оплати тільки використаних ресурсів.

Хмарні обчислення належать до додатків та послуг, що працюють в розподіленій мережі з застосуванням віртуальних ресурсів, доступ до яких можливий за допомогою мережевих технологій та протоколів Інтернету. Парадигма хмарних обчислень включає віртуальні ресурси та фізичні системи, на яких працює програмне забезпечення, абстрагуються від користувача.

Хмарні обчислення - інформаційно-технологічна концепція, що забезпечує мережевий доступу, на вимогу до обчислювальних ресурсів, таких як мережі передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів, які

можуть бути оперативно надані користувачу та звільнені з мінімальними експлуатаційними витратами.

1.2. Хмарні обчислення: труднощі та проблеми

Одна з головних проблем, якою стурбовані користувачі у послугах хмарних обчислень це переміщення конфіденційних даних і додатків з приватних обчислювальних середовищ у хмару, яка спільно використовується різними користувачами та яке зазвичай має загальнодоступну мережу. За результатами опитування, що було проведене у вересні 2009 року Міжнародною корпорацією даних (IDC), виявлено кілька проблем, що стосуються хмарних обчислень, як показано на рисунку 1.1 [5], безпека була визначена як найбільша проблема.

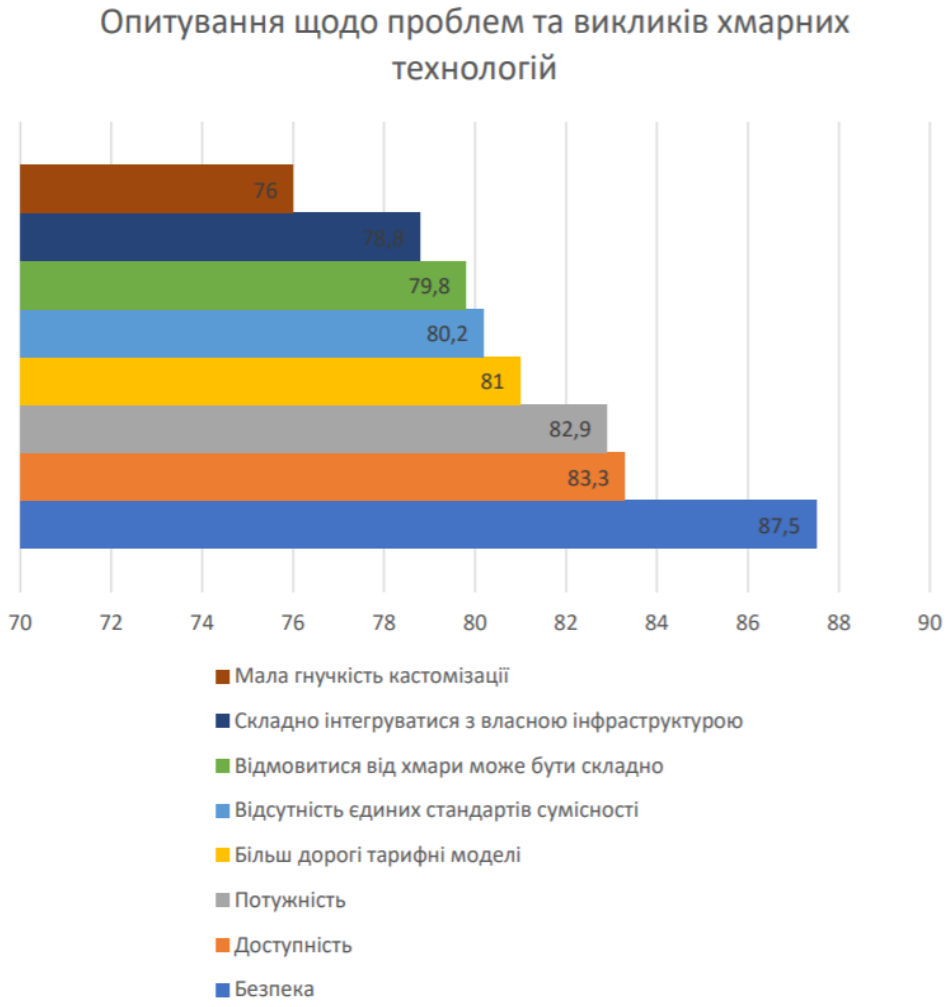


Рис. 1.1. Ранжування проблем клієнтами хмарних послуг [5]

Проблеми безпеки в хмарному середовищі зазвичай пов’язані з їх основними технологічними компонентами. Наприклад, веб-додатки, служби, віртуалізація та криптографічні методи. в даний час є найбільш поширеними методами для досягнення задовільного рівня вимог безпеки для хмарних обчислень.

Отже, будь-які вищезазначені відомі вразливості основних технологічних компонентів можна розглядати як вразливості хмарного середовища. Наприклад, протокол HTTP, який застосовуються в веб технологіях, піддається перехопленню сеансів та атакам сеансового рівня.

Віртуалізація - ще одна вразлива проблема для користувачів. Крім того, існують різні інші можливі вразливості, які можуть бути присутніми в хмарних обчислювальних системах, і вони пов’язані з його інфраструктурою. Вразливості в операційних системах та інших програмах, що реалізовані програмно і встановлені в хмарну інфраструктуру, також можна розглядати як такі, що пов’язані з вразливостями хмарних обчислень.

Нижче розглянуто конкретні вразливості безпеки, пов’язані з особливостями хмарних обчислень.

Несанкціонований доступ до інтерфейсу управління: в хмарних обчисленнях інтерфейси управління зазвичай доступні через загальнодоступні мережі для авторизованих клієнтів і можливих неавторизованих зловмисників, в той час як звичайні центри обробки даних як правило доступні тільки авторизованим адміністраторам безпосередньо або через приватні мережі. Також доступ до управління зазвичай здійснюється через веб-додаток або сервісні технології, тому інтерфейс управління хмарами, ймовірно, схильний до вразливості цих технологій.

Проблема відновлення даних: через віртуалізацію і спільне використання хмарних послуг на апаратному рівні області пам’яті і зберігання даних, що були орендовані попередніми користувачами, можуть бути перерозподілені. Є вірогідність, що нові користувачі можуть відновити дані з даних областей пам’яті та зберігання і отримати доступ до конфіденційної інформації.

Вразливість наявності шаблону віртуальної машини (рис. 1.2): нова віртуальна машина зазвичай створюється шляхом клонування образу шаблону

попередньо конфігурованої віртуальної машини для економії часу та зусиль. Таким чином, багато користувачів орендуватимуть віртуальні машини зі схожими конфігураціями. В такому разі зловмисник матиме доступ до інформації образу шаблонів хмарних систем, ставши користувачем хмари з правами адміністратора. Як тільки зловмисник отримує доступ до образів шаблонів, він може знаходити вразливості в цих образах.

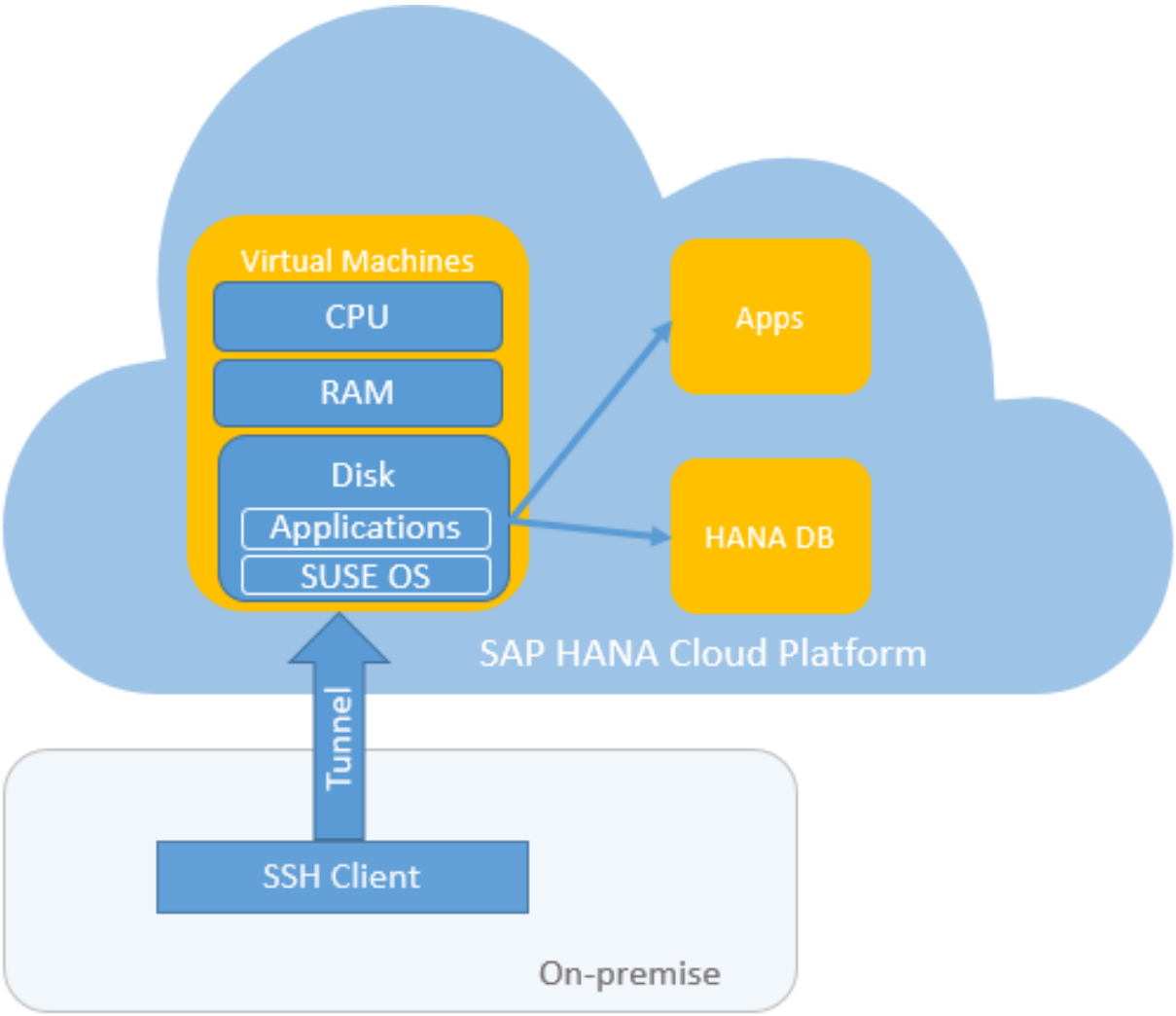


Рис. 1.2. Схема взаємодії віртуальної машини у хмарному середовищі на прикладі HANA Cloud Platform

Ін’єкційні вразливості: більшість хмарних сервісів використовують служби веб-додатків, тому, використовуючи вразливості в службах веб-додатків, можна вводити зловмисні коди в хмарну систему і, як результат, зламати веб-сервери, які обслуговують дані служби. Існує багато прикладів шляхів взлому з використанням

зловмисних кодів, таких як коди SQL, команда ОС або коди JavaScript. Як тільки веб сервер вийшов з ладу, він може використовуватися в якості стартового поля для зловмисника для взламування інших цілей в системі (бази даних, пераційні системи).

Показники безпеки і складнощі моніторингу: користувачам необхідно мати можливість вимірювати і контролювати ситуацію безпеки хмарних послуг і ресурсів (рис. 1.3.). Однак надання таких можливостей користувачам хмар як і раніше є проблемою, тому що доступні стандартні інструменти ще не підходять для хмарного середовища. Через те, що хмарне середовище має складні і динамічні ієрархічні сервіси, що можуть включати в себе різні провайдери хмарних обчислень, хмарне середовище вимагає оновлених розподілених можливостей моніторингу, відповідних цим характеристикам.

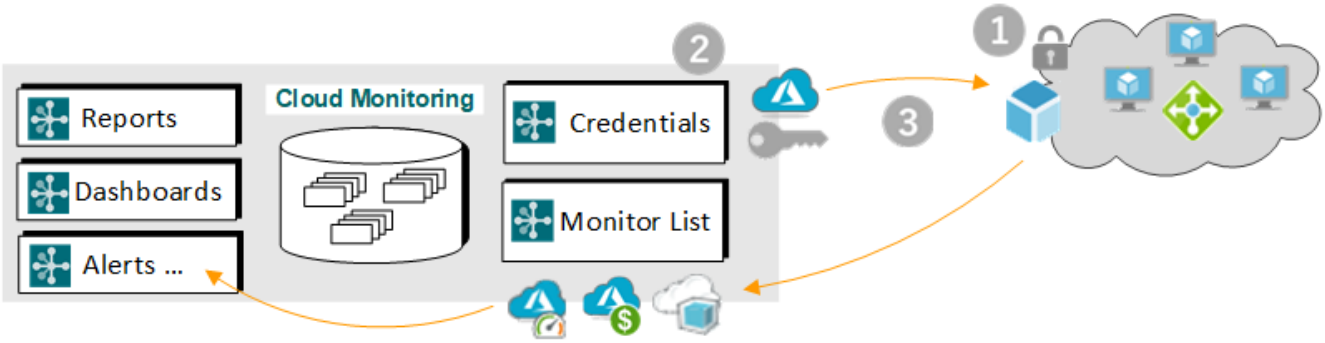


Рис. 1.3. Приклад завдання для інтегрованого рішення для моніторингу хмари WhatsUp Gold

Складність в управлінні цифровими ключами і випадковими числами: в хмарному середовищі існують різні типи ключів та випадкових чисел, що необхідні для криптографічних розрахунків. Управління та зберігання ключів в хмарному середовищі - одне з найважливіших завдань, оскільки відсутня повна фізична ізоляція між ресурсами зберігання, наданими для різних користувачів.

Ефективність генерації випадкових чисел в більшості випадків залежить від апаратного годинника, що використовується генератором випадкових чисел. Відсутність подібної ефективності може бути використане в хмарному середовищі, де в різних сеансах може бути кілька користувачів хмар, які застосовують однакові

ресурси генерації одночасно. Це може призвести до перевантаження ресурсів генерації випадкових чисел або отримання слабких чисел. Таким чином, впровадження традиційних механізмів безпеки, таких як модуль апаратної безпеки, що базується на ефективному ресурсі генерації випадкових чисел у хмарне середовище є складним питанням у забезпеченні безпеки у хмарному середовищі.

Функціональна сумісність хмари: ця проблема пов’язана з тим, як різні провайдери дозволяють користувачам безперешкодно переміщувати свої дані від одного провайдера до іншого і навпаки. Без функціональної сумісності між провайдерами, власник даних може заблокувати окремого провайдера і не матиме можливості швидко перейти до інших провайдерів або оптимізувати послуги між різними провайдерами.

Спостереження за шаблонами активності: шаблони активності одного користувача можуть спостерігатися іншими клієнтами або хмарним провайдером. Це спостереження може бути фактором для атаки або використано для виявлення дій, що не можуть бути виявлені у звичайних обставинах. Наприклад, обмін інформацією між двома різними компаніями може свідчити про планування злиття цих компаній.

Необхідність проведення аудиту компаній, підзвітність та надійність: в хмарному середовищі має будуватися довіра між провайдерами та користувачами. Прозорість роботи через високий рівень якості проведення аудиту та підзвітності має важливе значення для створення правильних відносин.

Відносини довіри ускладнюються, якщо хмарні провайдери делегують певні сервіси та послуги субконтракту. Користувачі хмарного середовища мають знати, чи існують які небудь субконтракти, що також можуть відповідати за дані або додатки. Одним з прикладів є Linkup, що надав онлайн-службу зберігання даних через стороннього провайдера під назвою Nirvanix [1]. Перед тим, як він завершив свою роботу в результаті втрати значної кількості клієнтських даних.

Розглянемо три найбільш поширені моделі використання хмарних технологій. Це є:

1. Software as a Service (SaaS)(«програмне забезпечення як послуга»);

2. Platform as a Service (PaaS)(«платформа як послуга»);
3. Infrastructure as a Service (IaaS)(«інфраструктура як послуга»).

SaaS-сервіси надають програмне забезпечення, що не вимагає завантаження та встановлення на персональні комп'ютери. Щоб скористатися необхідними функціями, дпотрібно відкрити онлайн ресурс.

SaaS має свої переваги, а саме:

1. Мобільність — хмарне програмне забезпечення встановлюється не на локальному пристрої, а на сервері. В результаті користувач може отримати доступ с будь якого пристрою та з різних локацій, де підключений до мережі Інтернет.
2. Актуальність — хмарне програмне забезпечення налаштовується швидко та просто. Також існує оновлення, тому користувачу завжди доступна остання версія ПЗ та можливість її оновлення до актуальної версії.
3. Доступність — програми, що включаються до моделі SaaS, зазвичай орієнтовані на вирішення базових та поширених завдань.

Отже, подібне програмне забезпечення зазвичай дешевше за звичайне ПЗ. SaaS-сервіс — це найбільш популярний тип хмарних технологій. Більшість користувачів ПК можуть їх використовувати. За функціоналом подібні ресурси нагадують звичні офлайн-аналоги.

PaaS – це повноцінні онлайн платформи з певним переліком інструментів та середовищем для розробки. Для звичайних користувачів ПК такі сервіси не є необхідністю. Основні користувачі PaaS сервісів - це інженери програмного забезпечення, для яких дана модель використовується для оптимізації процесу розробки, запуску та управління різними додатками.

PaaS являє собою проміжну ланку між SaaS та IaaS ресурсами. PaaS повноцінно забезпечує готове середовище розробки з базами даних, операційною системою та іншим необхідним користувачу чи проекту програмним забезпеченням. Це дозволяє інженерам одразу розпочати розробку, оскільки майже усі технічні складові процесу вирішені. Більшість PaaS [2] дуже підходять для розробки ПЗ.

Переваги хмарних платформ є очевидними, а саме:

1. Доступність — мінімізація початкових витрат, що в результаті виключає необхідність у великому обсязі початкових інвестицій.

2. Командна робота — на одній і тій самій платформі може працювати відразу певна кількість розробників або груп у реальному часі, що дуже пришвидшує процес розробки.

3. Простота — незважаючи на те, що PaaS-ресурси не призначені для звичйних користувачів, але ця модель хмарних технологій може бути використана навіть новачками. Ця особливість позитивно впливає на розвиток технологій та процесів розробки, дозволяє практично кожному створити власне програмне забезпечення.

Отже, PaaS-ресурси менш поширені, ніж SaaS. Їх використовують професійні користувачі досить вузьких сферах. Подібні ресурси мають перспективу витіснити та замінити стандартні інструменти розробки — за рахунок мінімізації витрат, адаптивності та доступності командної роботи.

IaaS - це апаратне забезпечення та ресурси, що розташовані безпосередньо у хмарі. Зазвичай це віртуальна альтернатива, створена за допомогою використання технологій віртуалізації. Поява IaaS [3] відкрила новий шлях для ведення бізнесу, надавши можливість компаніям зменшити витрати на підтримку IT-інфраструктури.

У випадку, якщо у компанії раптом з’являється необхідність у масштабних апаратних ресурсах, їй не обов’язково потрібно придбати додаткове обладнання за високу ціну — можливо лише використати ресурси хмарного сервісу. Звісно цей тип хмарних сервісів найменш поширений з усіх згаданих вище. Інфраструктура як сервіс мало цікавить звичайних користувачів, як правило, даною моделлю хмарних сервісів користуються системні адміністратори та мережеві архітектори.

Переваги моделі IaaS наведені нижче:

1. Значна економія на апаратному забезпеченні — у порівнянні з можливістю придбати апаратне забезпечення, налаштувати його та обслуговувати, оренда апаратного забезпечення потребує порівняно менші витрати ресурсів.

2. Незалежність від розташування — не має потреби у встановленні та

налаштуванні хмарної інфраструктури у кожній ситуації, коли компанія змінює локацію. Доступ до ресурсів у «хмарі» можливий з будь-якої точки розташування.

3. Гнучкість у використанні ресурсу — вибір оптимального пакету на певний період часу, можливість додати або вимкнути ресурси за необхідністю в будь який момент. Можливість вибору моделі оплати.

4. Захист — апаратні ресурси, що включає модель IaaS, зазвичай розташовані на різних локаціях, що можуть знаходитись навіть на різних континентах. Це зумовлює безперебійність роботи інфраструктури, навіть у ситуації виникнення непередбачуваних обставин.

У кожної із згаданих моделей хмарних сервісів — свій користувач. SaaS-ресурси орієнтовані на велику аудиторію користувачів персональних комп'ютерів, вони зручні, зрозумілі та доступні кожному. PaaS-хмари створені для спеціалістів у галузі IT, розробники програмного забезпечення та інші.

Користувачі моделі IaaS платформ – це зазвичай масштабні інтернет-компанії, мережеві та сервіс-провайдери. Більшість корпорацій інтегрують хмарні технології у своєму бізнесі на основі саме даної моделі. Розвитком подібних моделей є Business Process-as-a-Service (BPaaS) [4], що надає можливість постачальникам пропонувати горизонтальні або вертикальні сервіси бізнеспроцесів із застосуванням SaaS, створеного на вершині PaaS, IaaS.

1.3. Тенденції та напрямки рішень

Технологія хмарних обчислень (рис. 1.4.) стикається з різними проблемами, які неможливо вирішити традиційними рішеннями. Відповідний підхід має бути адаптований до конкретних характеристик сучасної обчислювальної парадигми. Дослідницькі шляхи вирішення проблем у хмарному середовищі різні в залежності від того, на яких видах хмарних питань зосереджуються дослідники.

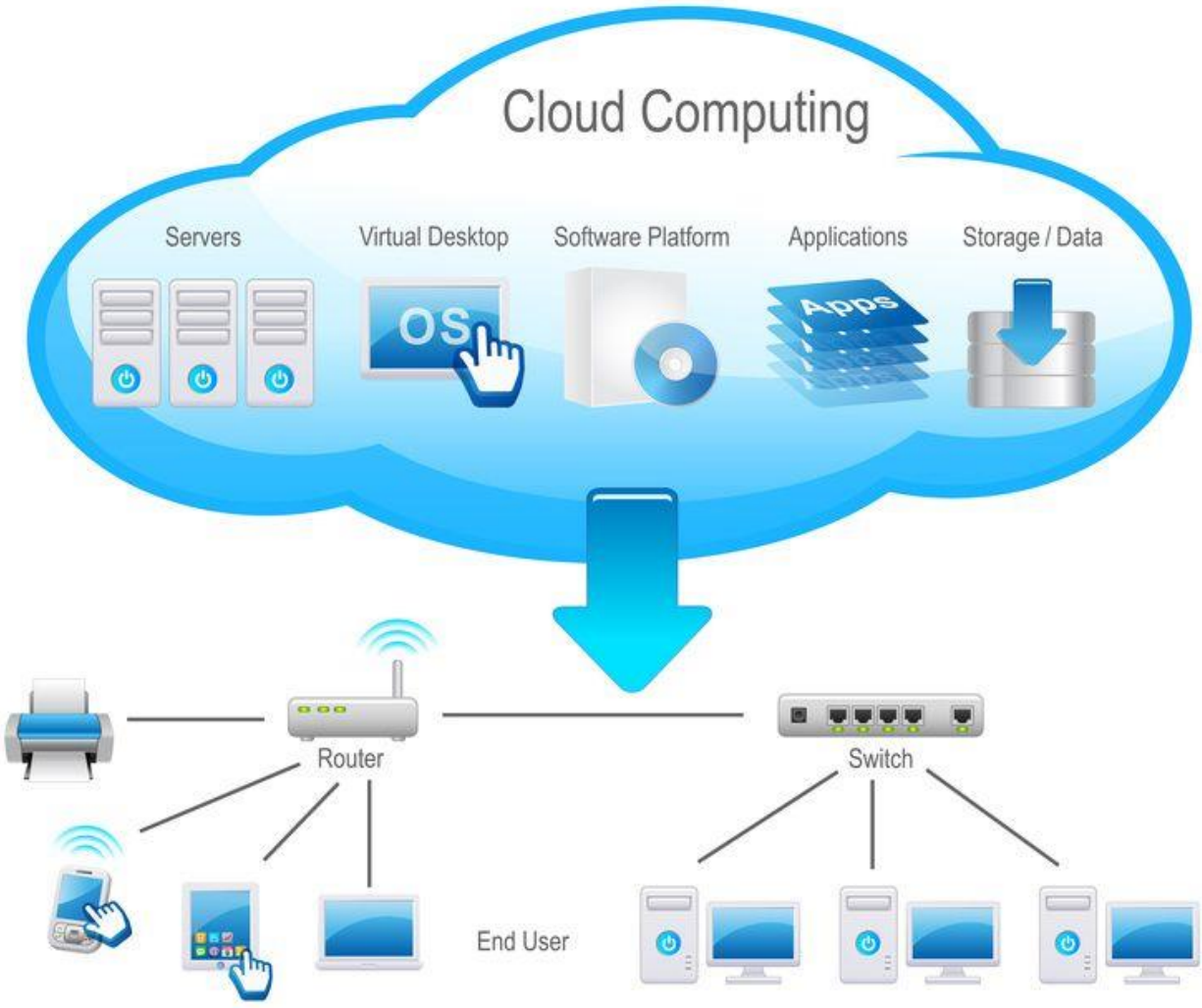


Рис. 1.4. Схема робота хмарних обчислень

На рівні віртуалізації технологій стверджується, що проблеми, що пов’язані з ізолюванням віртуальних машин на певній фізичній машині, потребують більшої уваги з точки зору безпеки та ефективності. Для високого рівня важливості, з приводу труднощів довіри у розрахунку на велику кількість клієнтів та вимог до можливостей аудиту в хмарному середовищі, можуть стати новими важливими завданнями. Однак, існує твердження, що конфіденційність і цілісність даних є основною вимогою безпеки.

Також в надійних або частково надійних хмарах сильним механізмом конфіденційності даних може бути ключ до встановлення надійності. Ненадійний сервер хмарних обчислень [5] в деяких випадках може надавати персональні дані і шаблони активності користувачів і повертати невірні дані від обчислювальних

процесів користувачам.

Також ймовірно, що ненадійний провайдер може здійснювати маніпуляції законним способом обробкою запитів користувачів в їх інтересах. Таким способом, захист даних, а саме їх конфіденційності та цілісності, як від провайдерів хмарних послуг, так і від зовнішніх спроб зловмисників призведе до створення більш сильних архітектур безпеки хмар, які сприятимуть більш широкому впровадженню хмарних сервісів.

1.4. Захист конфіденційності та цілісності даних від провайдерів хмарних середовищ

Конфіденційність і цілісність є одними з найважливіших вимогам для різних додатків. Клієнти хмарних обчислень не тільки стурбовані стосовно компрометації конфіденційності та цілісності своїх даних від можливих зловмисників, а й від потенційно зацікавлених до цього провайдерів хмарних середовищ. На жаль, порушення безпеки, за 2011 рік показують, що великі компанії, такі як Google, EMC/RSA, Sony, UK National Healthcare System (NHS) і Amazon EC2, усі стикалися з інцидентами безпеки.

В хмарному середовищі дані клієнтів передаються стороннім провайдерам, які можуть бути надійними або ненадійними. Термін ненадійний може використовуватися для наголошення на тому, що хмарному провайдеру не можна цілком довіряти. Ненадійний постачальники хмарних послуг може не змінювати дані користувачів, але вони можуть у пасивному форматі порушувати конфіденційність даних або, наприклад, приховано змінювати протоколи для своєї вигоди.

Тобто сервер провайдера хмарних обчислень можна розглядати [6] як чесний, але допитливий сервер. Отже, провайдер заслуговує на довіру в наданні послуг з точки зору доступності даних, дотримання базових вимог контролю безпеки і обробки дозволених запитів на збереження даних і повернення вірних результатів. Проте, також можливі зловмисні дії всередині хмари, що можуть виконуватися адміністратором або співробітником. Через масштабоване впровадженням хмарних

сервісів дослідники вивчають і розробляють нові методи, які зберігають конфіденційність і цілісність зовнішніх даних без тотальної залежності від провайдерів хмар для забезпечення вимог безпеки.

Подібні рішення мають надавати користувачам більше контролю над захистом своїх даних і можливість захищати дані від провайдерів. Через те, що сервер провайдера хмари, на якому розміщені певні дані, може бути не цілком надійним, існують методи вирішення таких ситуацій.

Загалом, запропоновані рішення базуються на шифруванні даних до того, як дані будуть відправлені на сервер провайдера. Хоча зашифровані дані захищені від несанкціонованого доступу, вони не можуть бути цілком корисними, якщо вони не дешифрувальні. Оскільки дешифрування даних в хмарі може розкривати їх серверам провайдера, то більш безпечно розшифровувати дані тільки в надійних машинах, що контролюються користувачем, авторизованим для доступу до цих даних.

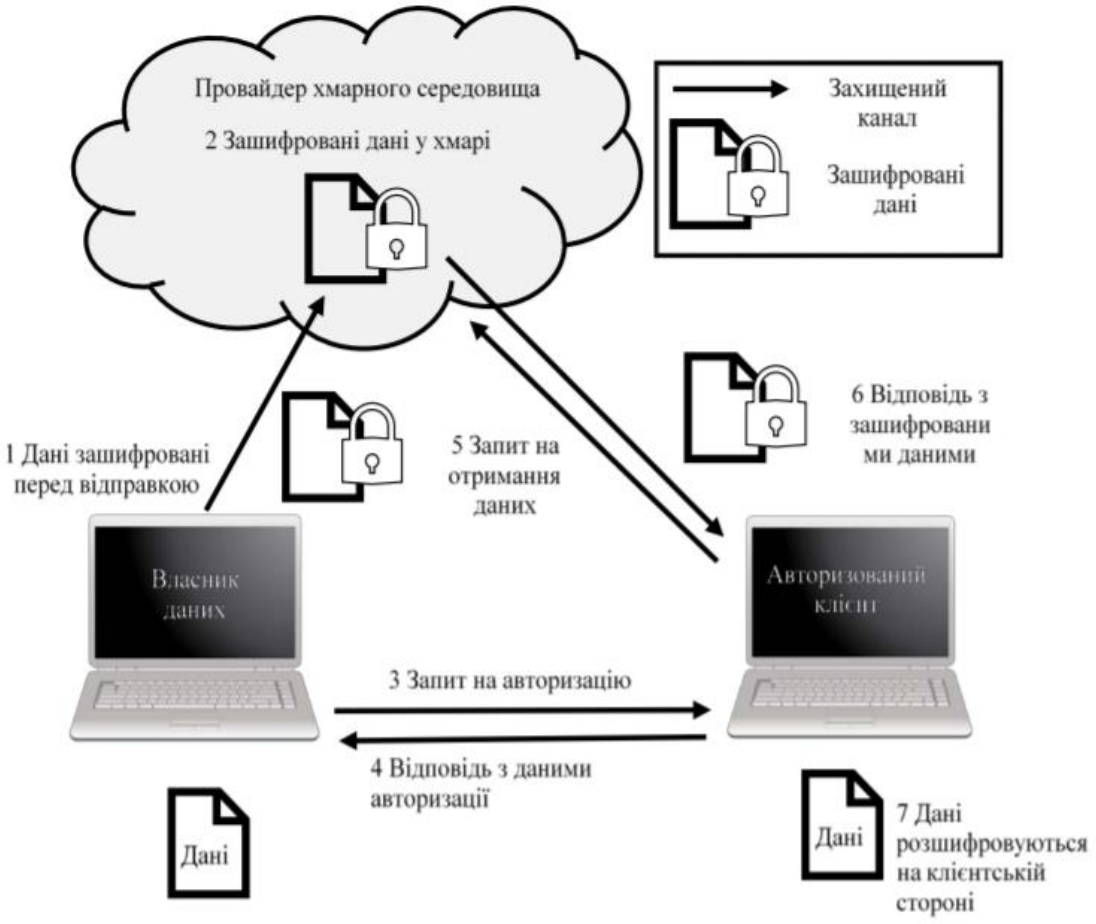


Рис.1.5. Базова архітектура для збереження конфіденційності даних в хмарі

На рис. 1.5. зображена базова архітектура шифрування даних для захисту конфіденційності інформації, перед відправкою їх у хмару [7]. Після цього дані залишаються зашифрованими, і тільки користувачі, авторизовані власником даних, мають можливість отримати облікові дані для доступу до зашифрованих даних. Зашифровані дані можуть бути розшифровані лише після їх відправки на авторизований комп'ютер користувача.

У такому сценарії конфіденційність даних не має залежності від припущення стосовно довіри сервера або індивідуальних угод про рівень послуг (SLA). Замість цього, захист конфіденційності повністю залежить від шляхів шифрування, що використовуються для кібернетичного захисту даних.

Решта проблем полягають у тому, як дозволити власнику даних і авторизованим користувачам ділитися і шукати зашифровані дані і використовувати їх для деяких обчислень відповідно до їх прав доступу. Всі ці функції повинні виконуватися безпечним чином, без розкривання приватної інформації неавторизованим суб'єктам, включаючи хмарних провайдерів. Сучасні криптографічні методи, схеми надійних обчислень орієнтовані на безпеку інформації в результаті можуть стати перспективним рішенням проблем безпеки у хмарному середовищі.

Криптографічні технології пристосовані до хмарної моделі. Нові технології криптографічного шифрування необхідні для того, щоб відповідати хмарній моделі і підвищити рівень безпеки інформації не змінивши при цьому зручність її використання (рис.1.6.). Якщо розглядати шифрування з можливістю пошуку, то зрозуміло, що це одна з областей[8], де розробляють можливість пошуку в зашифрованих даних без їх дешифрування. Лише авторизовані користувачі мають можливість запитувати та отримувати зашифровані дані, не відкриваючи при цьому приватну інформацію про дані та запит, що може містити певну інформацію про дані.

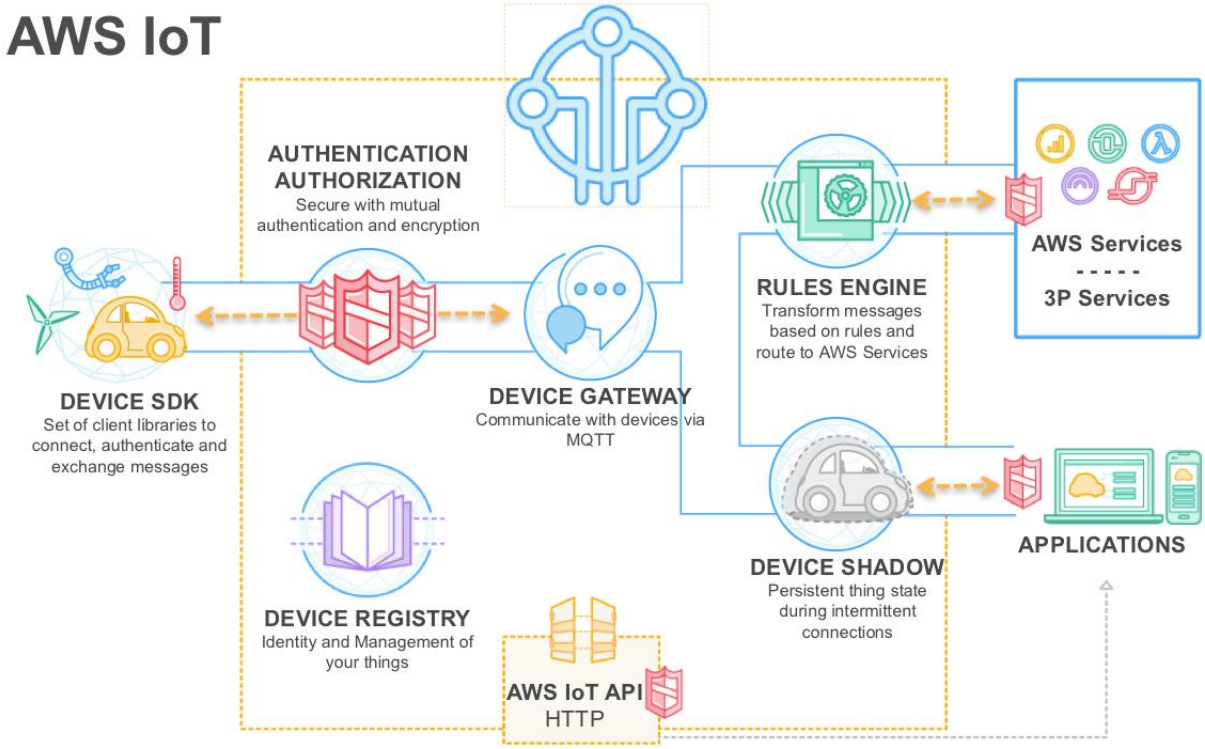


Рис. 1.6. Схема роботи хмари на прикладі хмари інтернету речей AWS IoT

Також існують методи шифрування, які дозволяють виконувати обчислення зашифрованих даних без їх дешифрування. Прикладом таких методів є гомоморфне шифрування. Інші методи шифрування, такі як шифрування на основі ідентифікаційної інформації (IBE) і шифрування на основі атрибутів (ABE) також можуть поліпшити управління ключами і контроль доступу до хмарного середовища.

Довіренні обчислення (TC)

IT-спільнота Trusted Computing Group (TCG), намагається зробити набір технологій, таких як автентифікація, управління паролями, шифрування даних, управління ідентифікацією та доступом, аби надати гарантії, що комп'ютерні системи виконуватимуть необхідний тип операції. TCG інтегрує схему довірених обчислень до Trusted Multi Tenant Infrastructure (TMI) [9], щоб встановити довіреність ненадійного середовища. Нова концепція націлена на те, щоб дозволити користувачам оцінювати довіреність хмарних провайдерів, застосовуючи набір апаратних і програмних технологій.

Підхід орієнтований на безпеку інформації

У стандартних методах захисту даних безпека забезпечується сервером, що зберігає інформацію. Методи для захисту даних і управління захищеними даними контролюються адміністраторами сервера. Такий системно-орієнтований підхід не підходить для захисту даних клієнтів в ненадійному хмарному середовищі. Для хмарних обчислень підхід орієнтований на безпеку інформації полягає в захисті даних зсередини, тобто дані, відповідно до їх значення та класифікації, мають певні вимоги безпеки, інтегровані у фактичні дані, щоб забезпечити захист даних на будь-якому етапі існування цих даних, незалежно від середовища, в якому вони зберігаються.

Висновки до розділу 1

Концепція хмарних обчислень у хмарному середовищі пропонує сучасну обчислювальну парадигму, в якій фізичні ресурси можуть спільно використовуватися користувачами в Інтернеті та де є можливість мати власний обчислювальний простір, використовуючи методи віртуалізації. Загальна концепція хмарних обчислень полягає в тому, що служби ІСТ та ресурси, що надаються ПХС через широкосмугові мережі, в основному в Інтернеті, і клієнти використовують ресурси та послуги за необхідністю та платять тільки за те, що споживають. Хмарні послуги постачаються в різних моделях, що базуються на послуги, що надається ІСТ.

Основними трьома хмарними послугами є: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS). Сьогодні існує п’ять моделей розгортання послуг хмарних обчислень, такі як приватна хмара, громадська хмара, публічна хмара, гібридна хмара та віртуальна приватна хмара.

В даний час модель публічних хмар є найпопулярнішою комерційною хмарною моделлю. Ця технологія надає великі переваги, такі як економічність, ефективність, економія часу та масштабованість. Але ця технологія стикається з низкою труднощів, тому проблеми з конфіденційністю та безпекою можуть вважатися найбільш складними.

Запропоновані рішення для підвищення рівня безпеки даних в хмарі мають

різні напрямки: деякі зосереджені на інструментах, таких як криптографічні алгоритми, інші зосереджені на більш комплексних рішеннях, що поєднують різні методи безпеки засновані на двох підходах: надійні обчислення (ТС) та підхід орієнтований на безпеку інформації (ОБІ).

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА

2.1. Рішення компанії CISCO щодо забезпечення кібернетичної безпеки хмарного середовища

Cisco - широко відомий бренд IT-корпорації Cisco Systems з США під яким у всьому світі випускаються мережеві маршрутизатори, комутатори, бездротові пристрої, системи відеонагляду. Діяльність компанії постійно масштабується та охоплює все більше і більше нових областей IT-галузі.

Cisco пропонує системи безпеки, телефонію на базі Інтернету, хмарні системи та інші рішення для спільної роботи і корпоративних мереж. Також компанія бере участь у розвитку Інтернету речей (IoT), проводить освітні програми і пропонує одну з багаторівневих і ретельних систем сертифікації інженерів комунікаційних технологій.

Компанія Cisco Systems [10], визнаний лідер в області мережевих рішень, пропонує також широкий вибір продуктів в області забезпечення інформаційної безпеки - від міжмережевих екранів і систем запобігання атак до засобів контролю вмісту, захисту різних додатків, систем індивідуального захисту серверів.

У кожній з цих областей компанія Cisco Systems [11] досягла результатів і займає перші місця на світовому ринку. Це було б неможливо без досліджень і розробок, на які щорічно витрачається близько 500 мільйонів доларів - більше, ніж заробляють в рік деякі інші постачальники ринку інформаційної безпеки.

Визначальним елементом стратегії хмарного провайдера має бути повне виконання нормативних вимог, це дозволить підвищити рівень безпеки і сконцентрувати ресурси на конкретних проектах з підвищення захищеності. Класичні заходи з управління ризиками будуть ефективні тільки з ростом бізнесу хмарного провайдера, коли управління ризиками буде направлено як на вибір контрзаходів і оптимізацію витрат, так і на підвищення прозорості бізнес-інфраструктури.

З технологічної точки зору захист хмарного провайдера в цілому схожа на захист віртуалізації в корпоративній сегменті, при цьому бажано використовувати практики вже побудованих систем. Наприклад, в загальнодоступних документах Amazon 200 сторінках [12] наводяться кращі приклади побудови захищеної інфраструктури, в тому числі класичні: сегментування мережі, відділення хмарної інфраструктури від мережі внутрішньої діяльності провайдера (кадрів, бухгалтерії і т.п.).

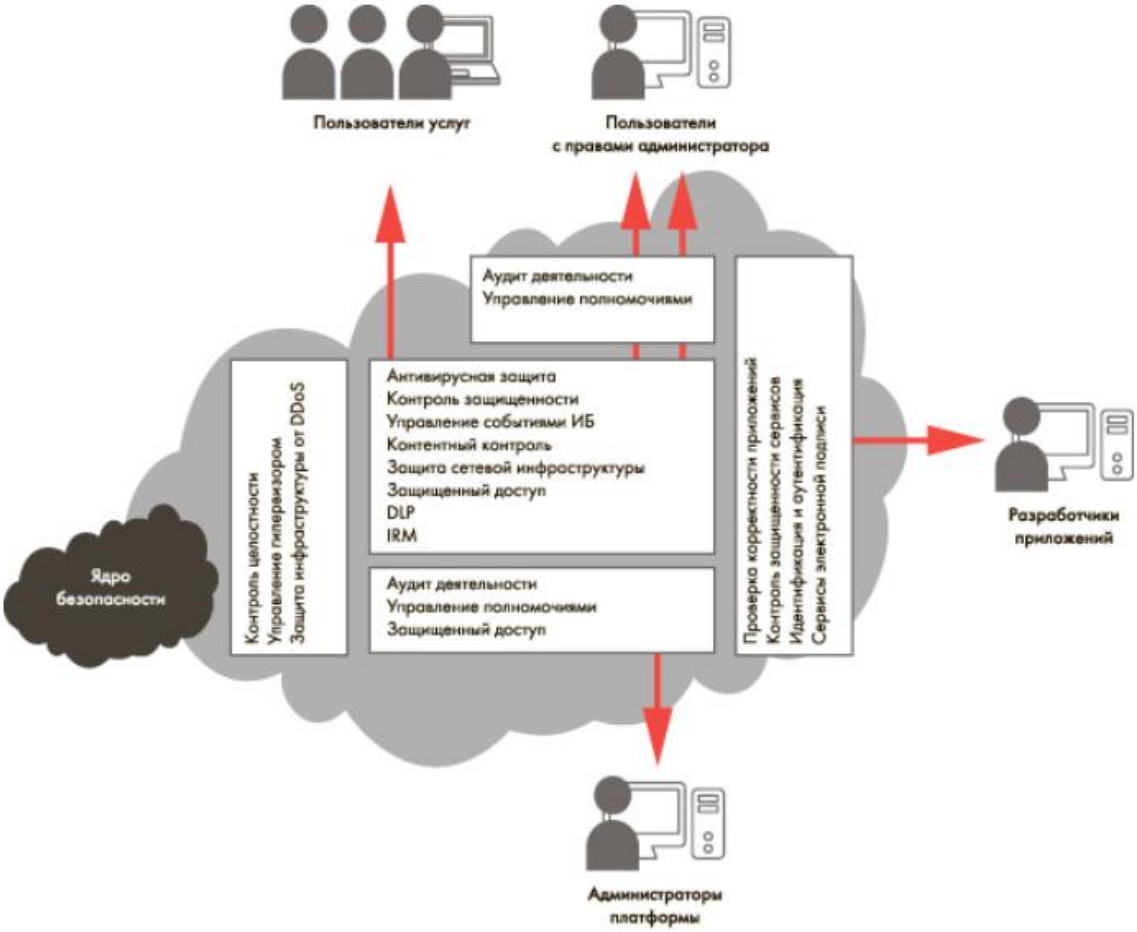


Рис.2.1. Приклад архітектури провайдера хмарних сервісів , архітектура ІБ національної хмарної платформи ВАТ «Ростелеком»

З точки зору забезпечення безпеки, хмари це лише один з різновидів інфраструктурних платформ, нехай навіть з високим ступенем автоматизації.

Зрозуміло, що в хмарі не обійтися без процесів, які добре зарекомендували себе в традиційних фізичних системах. Такі основні функції, як міжмережевий екран, IDS/IPS, віртуальне закриття вразливостей (Virtual Patching) та антивіруси, є обов'язковими елементами будь-якої концепції безпеки, будь то фізичні, віртуальні або хмарні системи. А ось завдання, що виникають при управлінні цими функціями, в різних інфраструктурах відрізняються[13].

Необхідно, щоб всі сервери з локальних, внутрішніх або зовнішніх хмар були ідентифіковані і інтегровані в концепцію управління безпекою. При використанні хмарних сервісів цього можна домогтися за допомогою прямої інтеграції з брокером хмарних сервісів, який в будь-який момент може надати інформацію про наявність різних хмарних серверів. Зіставляти вручну параметри експлуатованих серверів до вимог систем безпеки в динамічних середовищах неможливо, а при спробах такого порівняння виникають численні помилки.

Інтенсивний розвиток інноваційних процесів, поширення інформаційних технологій, їх інтеграція в усі сфери бізнес інтересів зумовило виникнення стратегічних проблем. Погіршується стан безпеки та з’являються випадки несанкціонованого втручання в роботу інформаційних та телекомунікаційних систем. Проблеми кібернетичного захисту інформації вимагають комплексного підходу, тобто побудови системи інформаційної безпеки (ІБ).

Сучасні підприємства підпадають під вплив факторів, що пов’язані із розвитком технологій, які спрощують процес роботи з великою кількістю інформації, однак це зумовлює проблеми, що пов’язані передусім з безпекою інформації. На початку розвитку хмарних технологій, підприємства, які були пов’язані з інформаційними технологіями, створювали умови для виникнення власних хмарних обчислень.

У 2007 рік Dell випускає свою версію хмарних сервісів, IBM запускає програмний продукт Blue Cloud. Через деякий час з’являються такі продукти, як Google’s MapReduce, Microsoftware’s Windows Azure, iCloud, Amazon CloudDrive тощо. Сьогодні завершується початковий етап розвитку хмарних технологій, які

полягають у новаторських експериментах, нестійких бізнес-моделях, невирішених питаннях інформаційної безпеки.

Інформаційна безпека підприємства – це життєво важлива складова захисту інформації, якою володіє компанія для уникнення несанкціонованого доступу, руйнування, модифікації та розкриття конфіденційності інформації. Під інформаційною безпекою мається на увазі захищеність інформації та підтримуюча інфраструктура, що забезпечує захист від випадкових та зловмисних дій, результатом яких може бути спричинення шкоди самій інформації, її власникам або підтримуючій інфраструктурі захисту інформації [1; 9].

Архітектура інформаційної безпеки охоплює різні процеси, технології, різні типи інформації, що підлаштовуються до них, враховуючи рівень складності та динаміку сучасного підприємства. Тобто вона описує очікувану структуру архітектури безпеки організації та інших, пов’язаних з безпекою інформації, складових та інтерфейсів.

Розвиток хмарних технологій спровокувала поширення масштабних розподілених систем для розробників програмного забезпечення. Хмарні системи зумовлюють просту й уніфіковану взаємодію між постачальником програмного забезпечення та його користувачем і включають сервісну підсистему, базу даних із відповідним доступом. Дані системи гнучко розподіляють обчислювальні ресурси реагуючи на запити про резервування ресурсу [14].

Під час інтеграції хмарних технологій програмне та технічне забезпечення пропонується користувачеві як Інтернет-сервіс. Користувач отримує доступ до власних даних, але не має можливості управляти і не має права налаштовувати інфраструктуру, операційну систему та програмне забезпечення, з якими проводиться робота. Хмарні сервіси трансформують підхід користувача до роботи з інформацією та програмами. Хмарні системи надають можливість мати доступ до інформації та серверів з будь-якої локації, звільнивши користувачів від потреби мати стаціонарний комп’ютер та зробивши можливою командну роботу багатьох людей одночасно.

Парадигма хмарних обчислень побудована на сучасній конфігурації. Нова конфігурація побудована із розмаїття оновлених технологій, таких як Hadoop (програмний каркас), Hbase (нереляційна база даних) сімейства Apache, що посилює продуктивність системи хмарних обчислень, але в той же час може призвести до ризику.

У хмарному середовищу користувачі реалізовують багато динамічних віртуальних організацій, що базуються на довірі між даними організаціями. Ризики часто утворюються на інтерактивних вузлах між віртуальними машинами і є гнучким, раптовим процесом. Середовище хмарних обчислень надає користувачеві можливість «придбати» повноцінний доступ до ресурсів, що також збільшує можливість ризику загрози безпеці інформації.

Вимоги до безпеки на базі аналізу HDFS HDFS (HadoopDistributed File System) є визнаною поширеною технологією хмарних обчислень, яка застосовується у великомасштабних хмарних обчисленнях у стандартній конфігурації розподіленої файлової системи.

HDFS нагадує існуючу розподілену файлову систему, таку як GFS (Google File System); вони мають схожі цілі, ефективність, доступність і стабільність. HDFS спочатку інтегрується у мережеву пошукову системі Apache Nutch [15] і стала базою проекту Apache Hadoop.

Аналізуючи HDFS, стандартні вимоги безпеки до хмарних обчислень можна розділити на кілька груп, а саме:

Перевірка правильності логіна клієнта: майже всі хмарні обчислення перевіряють браузер клієнта і здійснюють ідентифікацію користувача відповідно із запитом програм хмарних обчислень для первинної необхідності.

Присутність одиничної помилки з вузлом імені: якщо на вузол імені здійснюють атаку або зламують, це може призвести до найгірших наслідків у системі. Тому продуктивність вузла імені в хмарному середовищі його ефективність – це шлях до успіху в забезпеченні інформаційної безпеки. Підвищення захисту вузла імені є критично необхідним.

Швидке відновлення певних блоків даних і повний контроль за правом читання/запису: вузол даних або DataNode [16] – це вузол накопичення даних, де є ймовірність проблем та труднощів з доступом до даних.

Також потрібно враховувати різні можливості такі як контроль та управління доступом, шифрування файлів тощо.

Вся процедура захисту даних базується на конфіденційності, цілісності та доступності інформації. Конфіденційність належить до певної прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки.

Розглядаючи хмарне середовище дані зберігаються в центрах обробки інформації, де захист та конфіденційність даних неабияк важливі. Цілісність даних у різному вигляді не має значної ролі для підтвердження несанкціонованого пошкодження, зміни або порушення прав доступу.

Доступність даних означає, що користувачі мають можливість використовувати дані через використання потенціалу хмарних технологій. У склад моделі входить тришарова захисна архітектура системи, кожен шар виконує свої власні функції для забезпечення захисту інформації на всіх рівнях системи хмари.

Перший шар: аутентифікація користувачів цифрових сертифікатів [16], що видані відповідними органами; управління кодами доступу користувачів.

Другий шар: шифрування даних користувача, а також захист конфіденційності користувачів у відповідний спосіб.

Третій шар: використання інформації користувача для швидкого відновлення.

Захист усієї системи – це останній рівень даних користувача.

За допомогою трьох рівнів структури аутентифікація користувача інтегрується для забезпечення цілісності інформації [17]. Якщо в системі аутентифікації користувача відбулося неправомірне втручання і зловмисник входить в систему, шифрування файлів та захист конфіденційності інформації можуть забезпечити відповідний рівень захисту.

На даному рівні інформація користувача зашифровуються у ситуації, якщо ключ доступу був введений неправомірно. Через параметр захисту конфіденційності зловмисний користувач не зможе отримати повноцінного доступу до інформації, що є важливим для захисту важливих комерційних таємниць бізнес користувачів у хмарного середовища.

Отже, швидке відновлення шару файлів за допомогою відповідного алгоритму відновлення дає можливість інформації користувача швидко оновлюватися навіть у ситуації великих пошкоджень. Повний перехід до хмарних технологій вимагає серйозного підвищення вимог до якості надання двідповідних послуг доступу до мережі Інтернет, які стають неабияк важливими.

Найбільше у вирішенні цієї проблеми роблять успіхи американські провайдери. В американській практиці є традицією публікувати у повністю відкритому вигляді деталізовані обов'язки з наслідуванням високої якості надання послуг, які вказані в угодах про рівень обслуговування (Service Level Agreements) [15]. У ситуації, якщо оператор не виконує своїх зазначених обов'язків, він несе за це повну фінансову відповідальність.

Регулювання відносин у сфері хмарних технологій – непросте завдання, оскільки інтереси користувачів включають ціль у збереженні контролю та управління над своїми даними, інтереси постачальників хмарних послуг мають на меті максимальну свободу під час експлуатації та розширення своїх сервісів. Ці інтереси іноді розходяться у протилежних напрямах. Саме тому майбутнє бачення розвитку хмарних технологій багато в чому полягає у залежності від логічного компромісу обох сторін – як споживача, так і провайдера.

У дослідженні «Економіка хмарних обчислень» (The Economics of the Cloud) спеціалісти з компанії Microsoft [16] висловлюють думку, що традиційні правові проблеми зустрічаються у дослідженні будь-якої нової технології і через певний час юридичні перешкоди для хмарних технологій перестануть бути актуальними, оскільки ринок має властивість розвиватися.

2.2. Призначення, основні функції та склад програмного комплексу Cisco Cloudlock

Специфіка забезпечення ІБ хмарних сервісів полягає в тому, що підсумковий рівень інформаційної безпеки є сумою рівнів ІБ провайдера і клієнта.

Cisco Cloudlock - спеціальне рішення для хмари для безпечного доступу до такого середовища. Брокер дозволяє безпечно проводити операції в хмарі. Cisco Cloudlock націлений на захист користувачів, даних і додатків в хмарі. Надає можливість створити колективний рейтинг довіри для додатків і внесення їх в білий або чорний список в залежності від рівня потенційного ризику.

У рішенні Cisco Cloudlock впроваджений простий, автоматичний і відкритий підхід, який використовує API, для управління можливими ризиками у всій екосистемі. Брокер [1] бере на себе функцію боротьби з витоком інформації і одночасно контролює виконання всіх нормативів. Передбачено моніторинг «тіньових» IT-структур. За рахунок застосування сучасних алгоритмів, вдається на ранніх стадіях розпізнати аномалії поведінки та попередити можливу атаку. Рішення може ідентифікувати активність з країн, що не входять до «білого списку» і виконуються з підвищеною швидкістю.

Функція запобігання витоку даних DLP контролює хмарні середовища для захисту персональних даних і конфіденційної інформації. Використовується політика з широкими можливостями налаштувань для підприємств з різних сфер, масштабів, форм власності, в тому числі державної.

Cloudlock взаємодіє з такими середовищами, як Salesforce, Office 365, G Suite Dropbox і Box. Поряд з цим розглянутий продукт функціонує Вереd IaaS (Infrastructure as a Service), а також PaaS (Platform as a Service) і інтегрується з рішеннями таких постачальників засобів управління ідентифікаційної інформацією користувачів і управління доступом, як Okta, One Login і Cent rify, з метою пом'якшення наслідків підозрілої поведінки[17].

За словами Тернера з корпорації Ovum, служби, що дозволяють рішенням Cloudlock перевизначати списки управління доступом, відкликати права спільного

використання файлів або шифрувати файли і поміщати їх в карантин, виділяють це CASB-рішення на тлі продуктів інших постачальників.

На додаток до цього Тернер зазначив здатність пакету Cloudlock засвоювати аналітичні дані, що надаються його лабораторією, яка складається з колишніх співробітників розвідувальних служб Ізраїлю і США. Компанія Cloudlock, вміщена авторами підготовленого аналітичною компанією Gartner огляду 2018 CASB Magic Quadrant [18] в категорію нішевих гравців, увійшла також до групи фіналістів, які оскаржують призи SCMedia 2019 [19] за розробку кращого рішення щодо забезпечення безпеки обчислень в «хмарі».

У міру того як додатки, дані та ідентифікаційні дані переміщуються у хмару, групи по забезпеченню безпеки зобов'язані вміти управляти ризиками, пов'язаними з втратою контролю над традиційним периметром мережі. Зловмисники успішно користуються тим фактом, що складно одночасно захищати IoT і хмарні середовища, оскільки вони постійно розширюються та розвиваються.

Одна з причин пов'язана з відсутністю повної ясності в плані [20] того, хто ж фактично відповідальний за захист цих середовищ. Щоб вирішити ці питання, підприємствам необхідно комбінувати кращі практичні методики, вдосконалені технології забезпечення безпеки, такі як машинне навчання, і навіть деякі окремі експериментальні методології, в залежності від сервісів, якими вони користуються для свого бізнесу, і від того, як розвиваються загрози в цьому просторі.

Застосування алгоритмів машинного навчання дозволяє одержати більш докладне уявлення про хмарної активності користувачів, а не тільки число завантажень. Близько 23%, з проаналізованих користувачів компанією Cisco, було зазначено[21] в тому, що вони робили підозрілі дії по завантаженню більше трьох разів, зазвичай починаючи з невеликого числа документів. З кожним разом обсяг поступово збільшувався, і нарешті, у таких користувачів відзначався раптовий і значний сплеск завантажень.

Алгоритми машинного навчання дійсно здатні забезпечити кращий моніторинг хмари і поведінки користувача в ньому. Якщо спеціалісти кібербезпеки почнуть прогнозувати поведінку користувачів в плані скачування документів, вони

заощадять час, який можливо буде витратити на вивчення легітимного поведінки. Вони також зможуть запобігти потенційну атаку або інцидент з витоком даних до поді, якщо це станеться.

Згідно Порівняльному дослідженню Cisco рішень безпеки в 2018 році, обсяг використання інфраструктур [22] локальних і публічних хмар (рис. 2.2) зростає, хоча багато організацій все ще використовують локальні мережі.

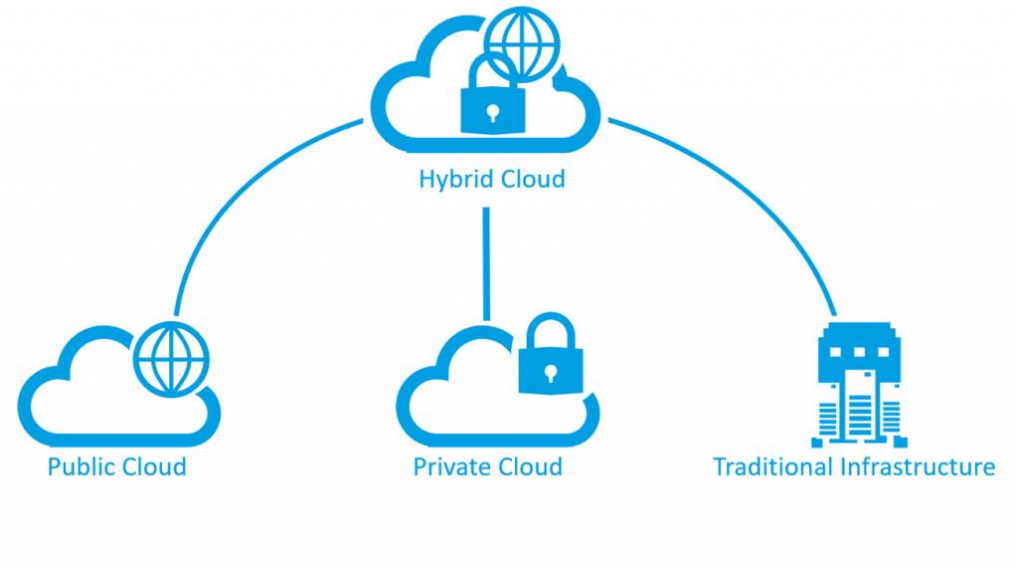


Рис. 2.2. Різновиди хмар (публічна, приватна, гібридна)

У дослідженні 2017 року 27% опитаних фахівців з безпеки сказали, що використовують зовнішні приватні хмари, в той час як в 2016 році їх частка становила 25%, а в 2015 - 20% (рис. 2.3). П'ятдесят два відсотки повідомили, що їх мережі розміщені на локальній приватній хмарі.

Cisco Cloudlock пропонує рішення брокера безпеки доступу до хмарної середовищі (CASB), що допомагають організаціям використовувати хмару безпечним чином. забезпечуючи наочність і контроль користувачів, даних і додатків для середовищ «програмне забезпечення як послуга» (SaaS), «платформа як послуга »(PaaS) і« інфраструктура як послуга »(IaaS). Також компанія забезпечує корисний аналіз кібербезпеки завдяки власним центру CyberLab з фахівцями, а також аналіз безпеки за принципом краудсорсингу.

Рис. 2.3. Порівняльне дослідження Cisco в галузі безпеки за 2018 р.

Cisco Cloudlock пропонує рішення брокера безпеки доступу до хмарної середовищі (CASB), що допомагають організаціям використовувати хмару безпечним чином. забезпечуючи наочність і контроль користувачів, даних і додатків для середовищ «програмне забезпечення як послуга» (SaaS), «платформа як послуга »(PaaS) і« інфраструктура як послуга »(IaaS). Також компанія забезпечує корисний аналіз кібербезпеки завдяки власним центру CyberLab з фахівцями, а також аналіз безпеки за принципом краудсорсингу.

Cisco Cloudlock забезпечує крос-платформне аналітику поведінки користувачів та суб'єктів (UEBA) [23] для SaaS, середовища IaaS, PaaS та IDaaS. Cisco Cloudlock використовує вдосконалене машинне навчання, алгоритми виявлення аномалій на основі таких факторів, як діяльність поза білим списком

країни та дії на відстані з неможливою швидкістю. Схема роботи Cisco Cloudlock є оптимальною (Рис. 2.4).

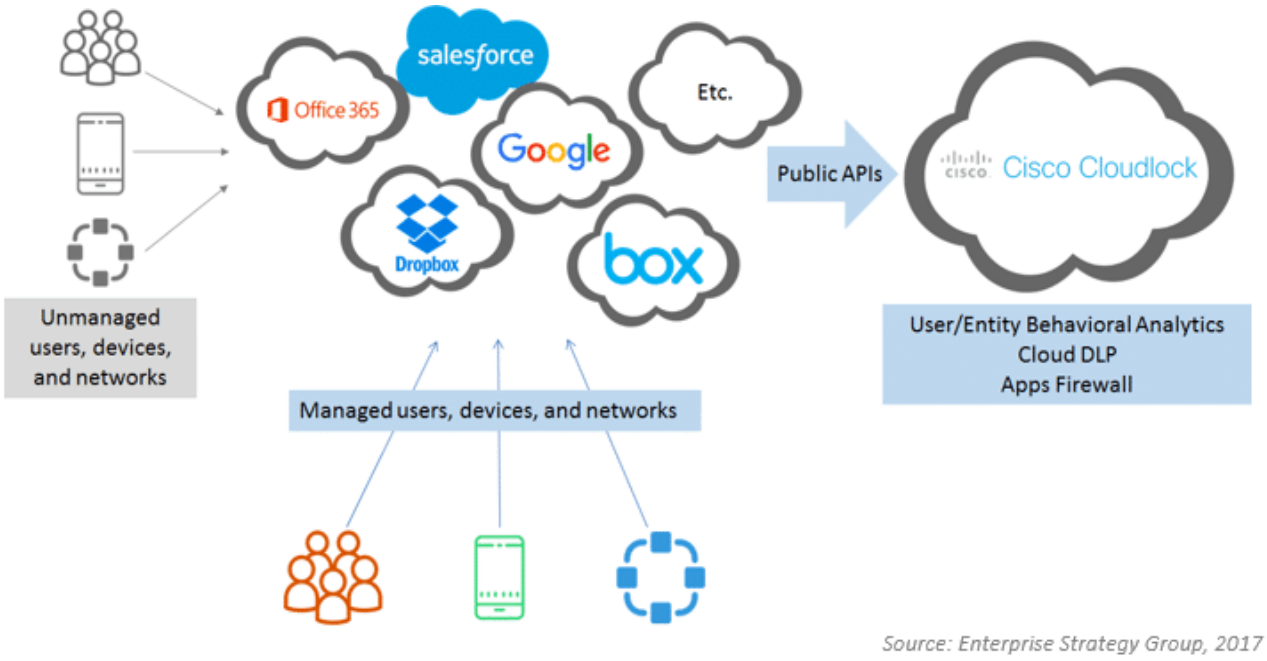


Рис. 2.4. Схема роботи Cisco Cloulock

Зловмисники перемагають сьогоднішні засоби безпеки, які спираються на периметр мережі, брандмауери, або орієнтуватися виключно на певну платформу. Діяльність на різних платформах не пов'язана, ускладнює або неможливо виявити підозрілі моделі поведінки. В той самий час, команди безпеки завалені попередженнями, які не мають пріоритету, корисної інформації чи контексту. Зіткнувшись з потоком непотрібних попереджень, законні порушення безпеки залишаються поза увагою.

Це проблема посилюється за рахунок використання хмарних додатків та платформ як організацій часто не бачать діяльності своїх користувачів у своїх SaaS, PaaS, IaaS та IDaaS середовищах.

Проблеми, які вирішує Cisco Cloudlock:

1. Відсутність видимості конфіденційних даних у хмарних додатках

Все більша кількість організацій застосовує хмарні програми. Видимість локальних систем DLP обмежена мережевою трафіку і не поширюється на хмарне середовище, таке як програмне забезпечення як послуга (SaaS) [24]. До того ж,

враховуючи легкість, з якою користувачі можуть розповсюджувати інформацію в хмарних середовищах і дуже високо спільний характер, поширення конфіденційної інформації до зовнішньої партій легко для співробітників, але аналітикам безпеки важко виявити.

2. Хмара як засіб вилучення даних

Кіберзлочинці та зловмисні особи можуть легко використовувати хмару служби доступу та проникнення конфіденційної інформації. Cisco Cloudlock дозволяє аналітикам безпеки отримати контроль над хмарними програмами та надміру відкрита інформація для боротьби зі зловмисною поведінкою.

3. Інтенсивні інструменти безпеки кидають виклик безпеці командних ресурсів

Традиційні засоби захисту даних вимагають великих ресурсів і вимагають великих значень угода з ручним наглядом через надмірні помилкові спрацьовування та обмежена автоматизована відповідь[25]. Крім того, проблеми розгортання та масштабованості вимагати додаткових ресурсів безпеки для досягнення мінімальної вартості. Ключові функції:

1. Аналіз поведінки користувачів та організацій

Cisco Cloudlock виявляє активність, яка свідчить про компрометацію облікового запису, співвідносячи та аналізуючи інформація про використання в середовищах SaaS, IaaS, PaaS та IDaaS (рис. 2.5) для виявлення аномалій. Крім того, завдяки вдосконаленому машинному навчанню, Cisco Cloudlock адаптивно вивчає поведінку користувачів розкрити підозрілі моделі поведінки. Крім того, Cisco Cloudlock інтегрується з IDaaS рішення для аналізу поведінки входу в систему для тисяч програм, підключених до цих служб.

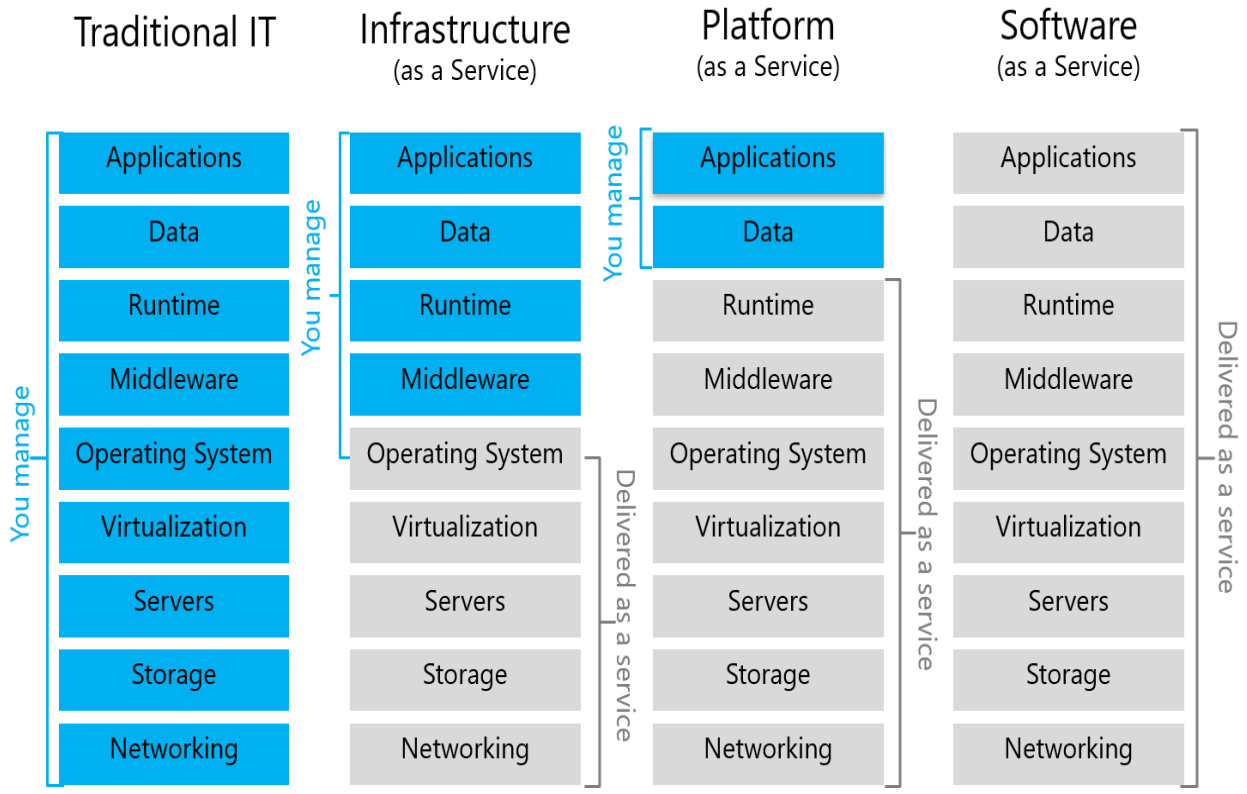


Рис. 2.5. Моделі хмар

2. Правозастосування на основі політики

Cisco Cloudlock визначає підозрілу поведінку, таку як користувацький для одного користувача вхід із географічного входу різне розташування за короткий проміжок часу, незвично великий обсяг завантажень файлів та доступ поза типовими тригерами робочого часу.

Крім того, Cisco Cloudlock дозволяє білий і чорний списки певних IP-адрес та діапазонів IP [26] для захисту від облікового запису компроміс. Коли виявляються аномалії, Cisco Cloudlock включає ряд автоматизованих заходи щодо виправлення, включаючи адміністративне попередження, сповіщення кінцевого користувача та навіть вимагання поглиблена автентифікація завдяки інтеграції з рішеннями IDaaS(рис. 2.6.).

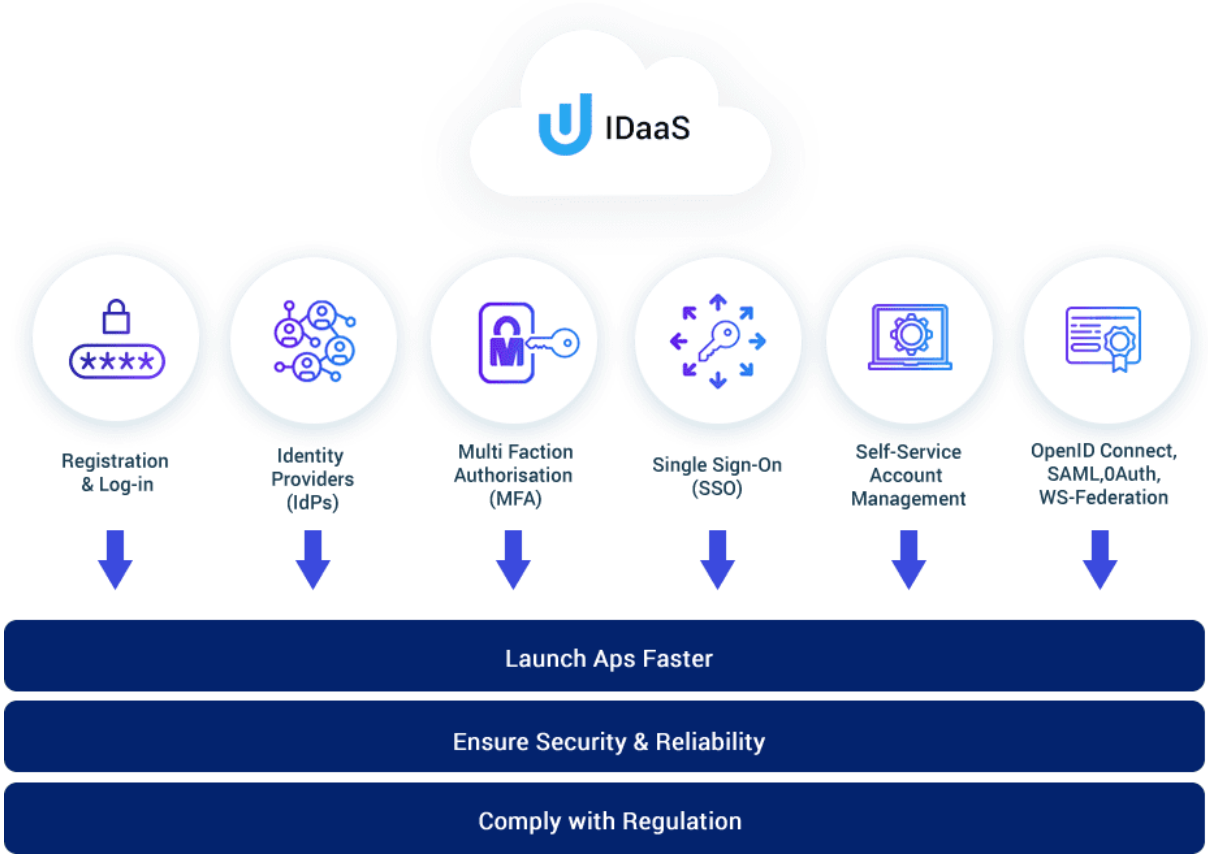


Рис. 2.6. Схема характеристик IDaaS

3. Захист від загроз

Cisco Cloudlock інтегрується зі службами виявлення шкідливого програмного забезпечення та емуляції загроз для виявлення шкідливе програмне забезпечення, яке постійно перебуває у хмарі, і ввімкнути автоматизовані робочі процеси реагування на загрози, включаючи адміністративні попередження [27], сповіщення кінцевого користувача, карантин файлів тощо. Cisco Cloudlock також має білий і чорний списки діяльності як з конкретних географічних регіонів, так і з діапазонів IC для додаткової впевненості у безпеці.

2.3. Реалізація технології забезпечення кібернетичної безпеки хмарного середовища в рішенні Cisco Cloudlock

Типові рішення платформи Cloudlock CASB безпеки працюють шляхом захисту периметра мережі, захисту трафіку в мережі і управління мобільні

пристрої. Ці рішення важливо мати, але у них є сліпа пляма: хмарні додатки, які з'єднуються з локальними програмами та даними, а також з іншими хмарними додатками. Некеровані користувачі, пристрої та мережі створювати уразливості, які ці рішення не бачать.

Cloudlock автоматично виявляє хмарні додатки, підключені до вашої середовищі, забезпечуючи видимість того, що додатки, до яких підключені користувачі, і то, як вони використовують і обмінюються даними. Це допомагає організаціям контролювати додатки за допомогою класифікація і моніторинг дій та відкликання доступу при необхідності.

Cloudlock відстежує всі дії користувачів, які відбуваються в будь-якому виявленому хмарному додатку і підключається до загальнодоступних API кожної хмарної платформи. Коли користувач завантажує файл в Dropbox [22], наприклад, Dropbox записує цю подію і передає його Cloudlock через API; Cloudlock потім може сканувати контент за допомогою попередньо налаштованого механізму класифікації, оцінити його в контексті налаштованих політик, визначити, порушення, і негайно відреагувати, зашифрувати їх або помістити файл в карантин.

Також інтеграція з іншими інструментами дозволяє проводити детальну експертизу після атаки. Cloudlock відстежує дії керованих і некерованих користувачів, пристроїв і мереж.

Хоча багато хмарних додатків пропонують засоби управління безпекою, вони не можуть забезпечити цілісне уявлення про всі додатки з сторона користувача; наприклад, Google і Dropbox можуть відображати дії користувачів, але IT-адміністратори не можуть зіставити інформацію між ними, а тим більше в тисячах додатків, які сьогодні використовує більшість організацій.

Cloudlock забезпечує цілісний погляд, це відкрите рішення, легко інтегральне з існуючими рішеннями мережевої безпеки, SIEM, EMM і IAM (рис. 2.7.), воно може також використовувати журнали інших CASB, щоб розширити видимість.

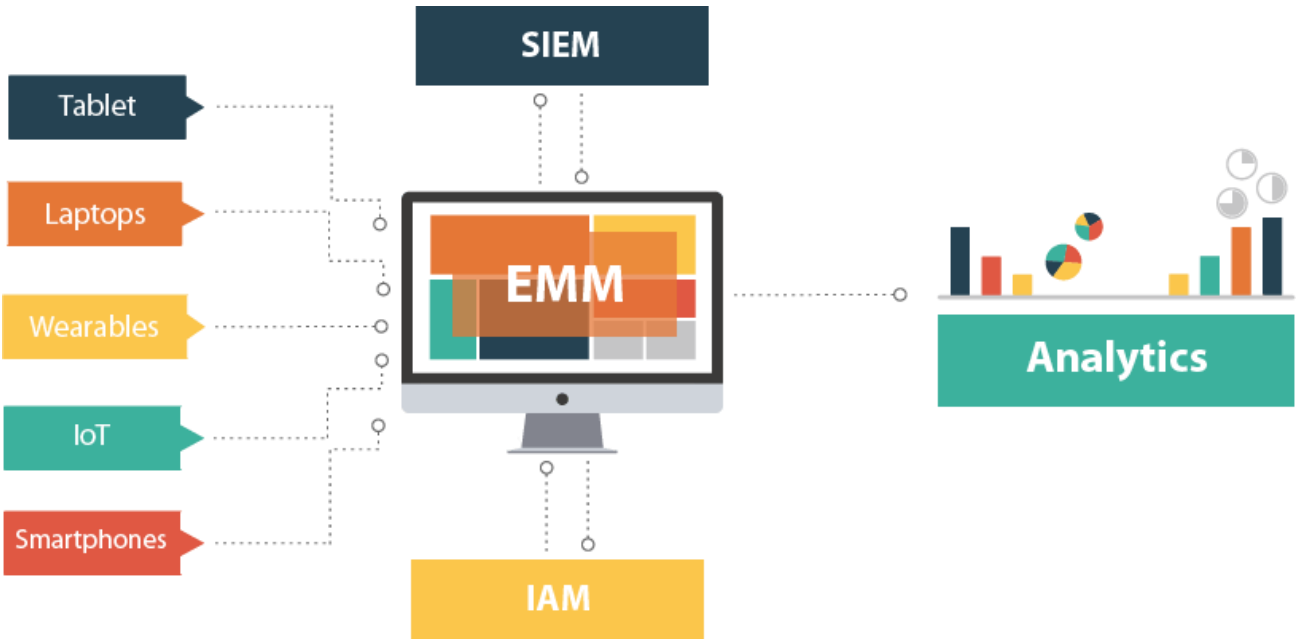


Рис. 2.7. Існуючі рішення безпеки, що інтегруються з Cloudlock

На відміну від рішень CASB (рис.2.8) на основі шлюзів, Cloudlock не встає між користувачами і їх хмарними додатками. Він знаходиться в AWS, поряд з іншими хмарними додатками, відстежує дані в режимі реального часу і в стані спокою.

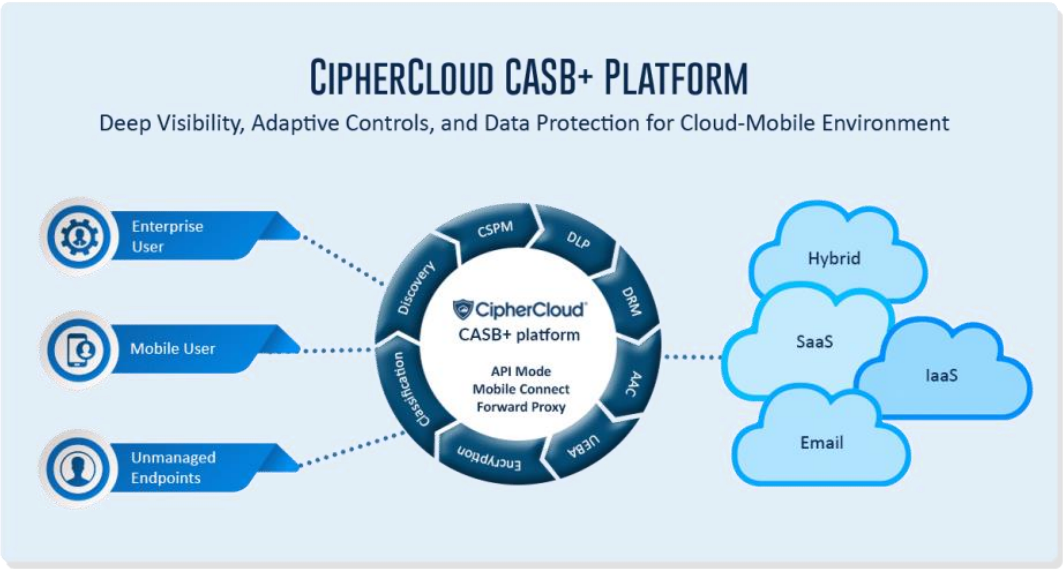


Рис. 2.8. Схема роботи CASB

В результаті дії Cloudlock не впливають на продуктивність або масштабованість так само, як проксі або шлюзи. Це також дозволяє нове розгортання Cloudlock забезпечити видимість того, які дані використовувалися і як вони передавалися в минулому, а не тільки з моменту розгортання, як з CASB (рис. 2.9), не заснованими на API.

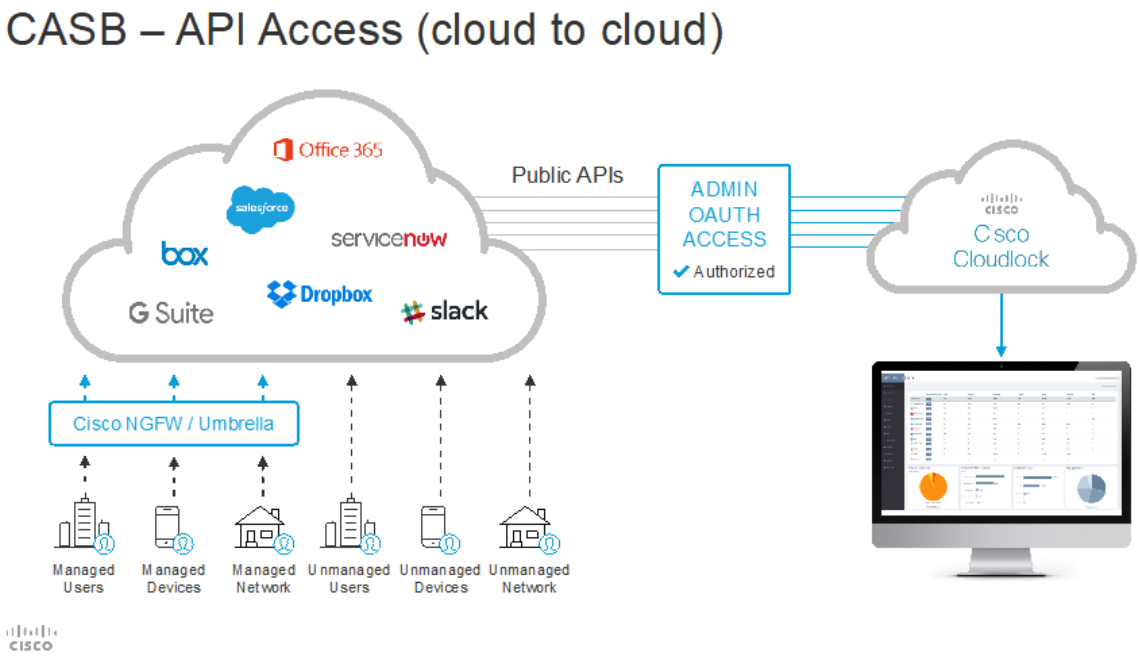


Рис. 2.9. CASB – API Access (хмара - хмара)

Cloudlock налаштовується швидко і легко, не відволікаючи користувачів. Він складається з набору мікросервісів, наприклад для даних, класифікації або захисту від загроз. Мікросервіси доступні через призначений для користувача інтерфейс Cloudlock або через API для інших продуктів. Програмне забезпечення поставляється з більш ніж 80 зумовленими політиками (рис. 2.10), які можна налаштувати в міру необхідності, наприклад, для визначення рівня чутливості, підходяща близькість даних, розкриття даних або політики по відділах.

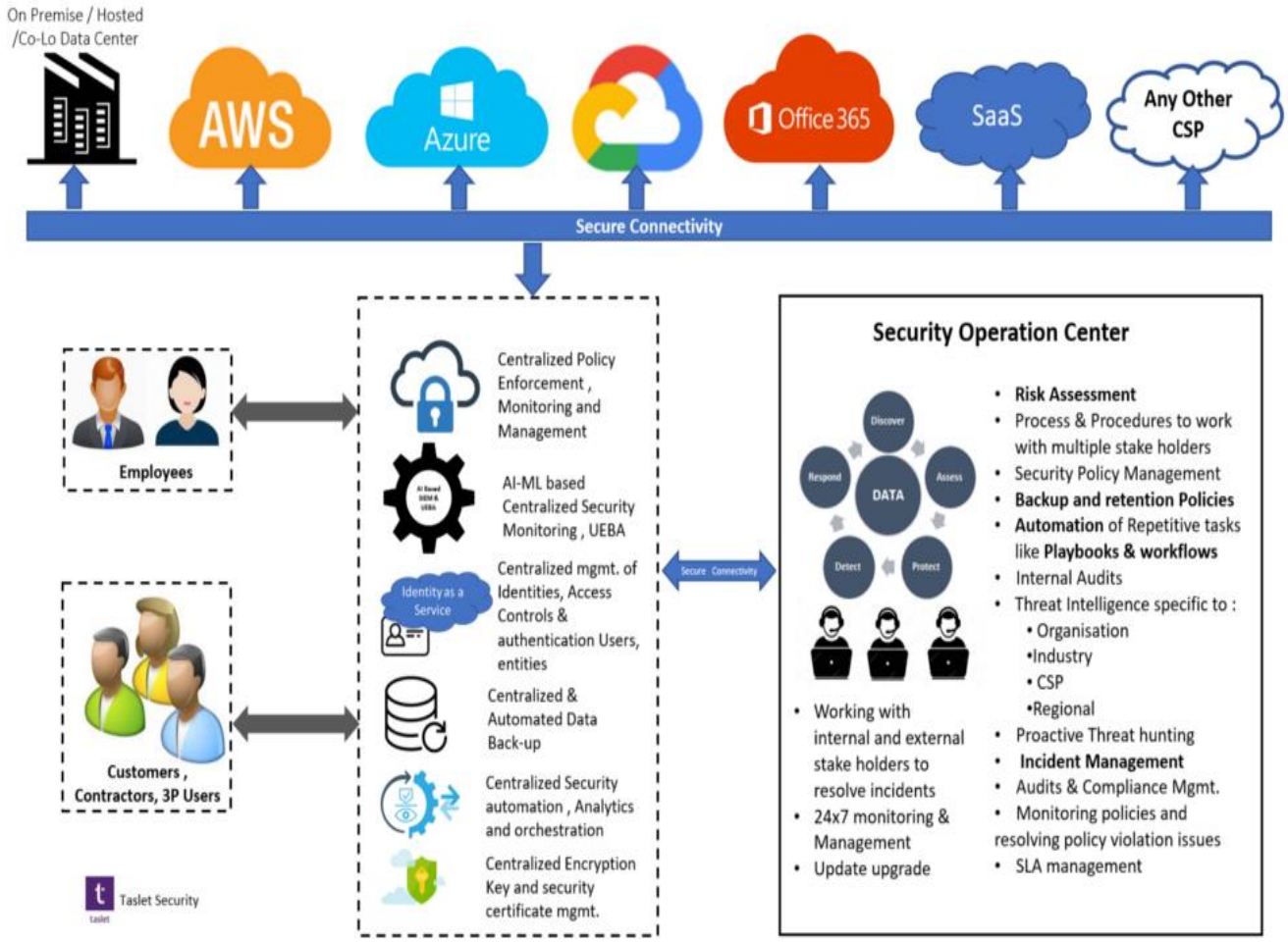


Рис. 2.10. Операційний центр безпеки у хмарні системі

Наприклад, організація може дозволити хмарним додаткам зберігати один номер кредитної картки, але ідентифікація сотень з них може викликати попередження і дії. Деталізовані політики можна створювати і розгортати в кількох хмарних додатках, позбавляючи адміністраторів від необхідності налаштовувати індивідуальні політики (рис. 2.11) згідно з додатками.

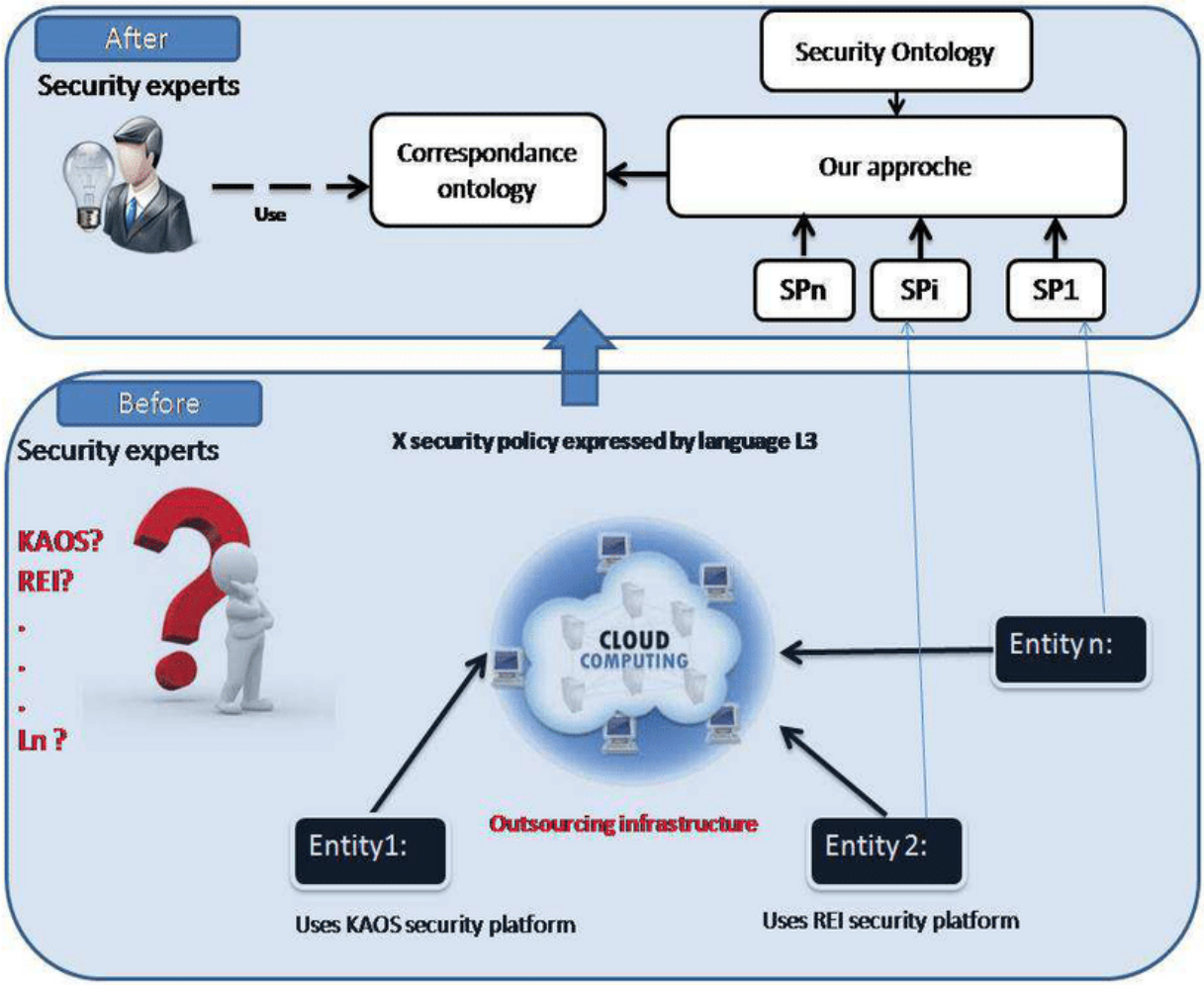


Рис. 2.11. Приклад співвідношення політик безпеки та їх реалізації

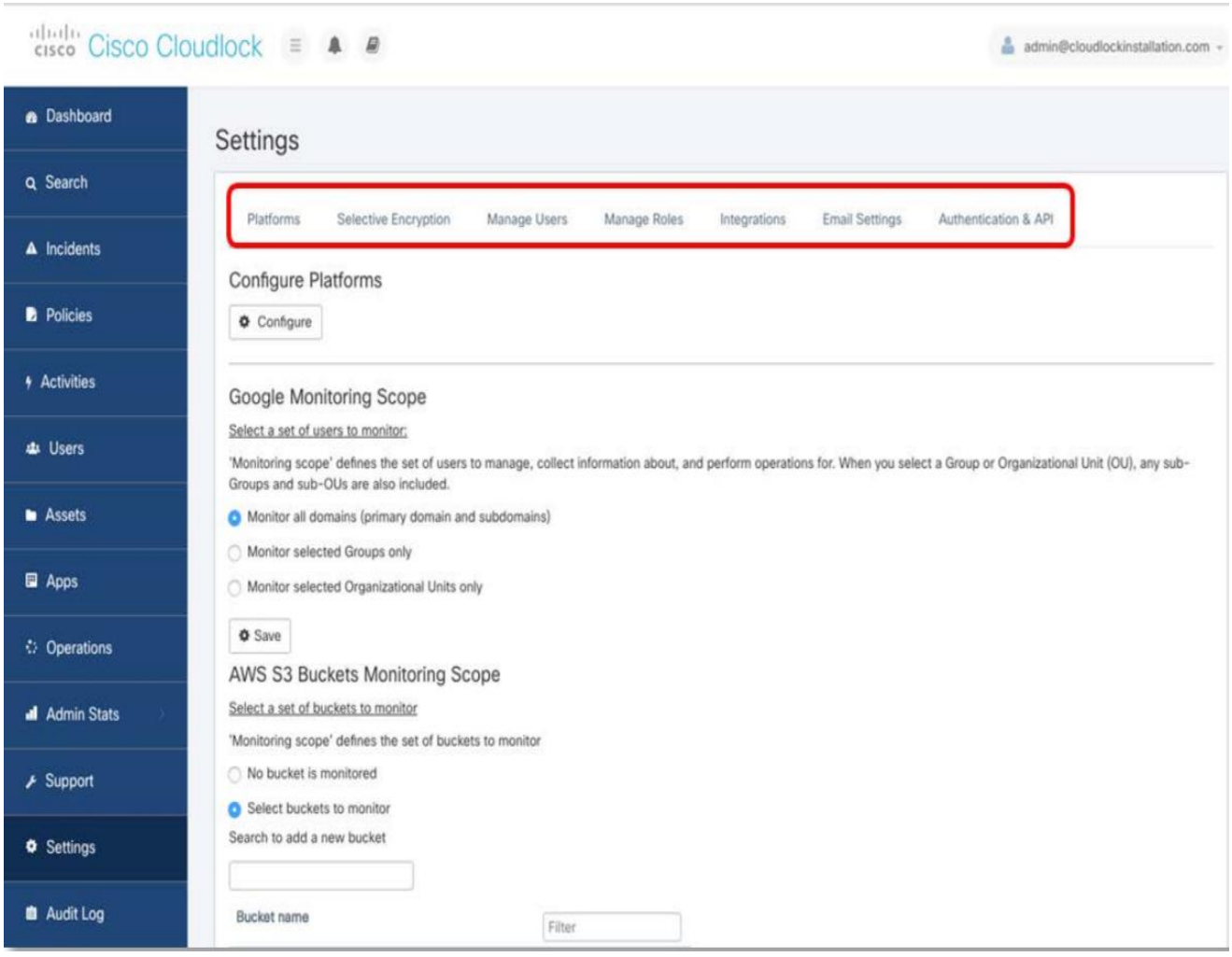
Політики можуть застосовуватися до користувачів індивідуально або в групах в залежності від поведінки, місця розташування та IP-адреси. Cloudlock відстежує дії користувачів і може переглядати журнали Office 365, Google, Dropbox, Box, Salesforce або інших хмарних додатків через API [14].

Можна створити політики, які будуть діяти автоматично при виникненні подій, наприклад, автоматичний відгук токен OAuth і відключення з'єднання для заборонених додатків або автоматичне шифрування і приміщення в карантин

даних, таких як коли номер кредитної картки додається там, де його бути не повинно.

ESG Lab провела практичну оцінку функцій безпеки додатків Cloudlock за допомогою демонстраційної середовища. тестування зосереджені на простоті використання, наочності і захисту підключених хмарних додатків. Середовище включає хмарні додатки для спільної роботи / продуктивності (Office 365, Slack), обміну файлами (Dropbox, Box), хмарного сховища (Google Drive, AWS), CRM (Salesforce), управління IT-послугами (ServiceNow) і ідентифікація / єдиний вхід (OneLogin, Okta).

Налаштування Cloudlock відбувається в рамках вже розгорнутого середовища Cloudlock, тому ESG Lab почала вивчення варіантів конфігурації. На вкладці «Налаштування» ESG Lab [4] можна легко управляти платформами, шифрувати файли, додавати і видаляти користувачів і ролі, управляти інтеграцією



з іншими додатками, такими як безпека Cisco Umbrella DNS, а також керувати логінами SSO і токенами API (рис.2.12).

Рис. 2.12. Інтерфейс налаштувань Cloudlock

Наприклад, Cloudlock може відстежувати всі або вибрані домени Google і організаційні одиниці (OU), певні сегменти AWS S3, канали Slack і домени Office 365, Box і Dropbox. Панель управління Cloudlock пропонує високорівневе уявлення про те, що відстежує Cloudlock: поведінка, дані і додатки. Кожна вкладка включає в себе звіт верхнього рівня з чотирма ключовими статистичними даними за минулий тиждень, які можуть вказувати на порушення або витік даних.

Ці зведені вкладки об'єднують деталі, які також можна переглянути на вкладках меню зліва. Вони можуть відразу попередити адміністраторів про потенційно небезпечному доступі до середовища.

Кожна вкладка включає додаткові докладні відомості та діаграми, що зв'язують аномальні дії з рівнями ризику, хмарними додатками, користувачами і місцями розташування. поведінкові та Виберіть Data Risk містять діаграми і графіки, що показують лінії тенденцій, схильність активів в залежності від хмарної платформи та місцезнаходження, а також докладну інформацію про активність активів і завантаження по користувачах. Адміністратори можуть натискати на стовпці графіків, карти і ідентифікатори користувачів, щоб навіть надалі.

На панелі управління ризиками (рис. 2.13) додатків показані важливі деталі для оцінки рівнів ризику хмарних додатків. У лівому верхньому кутку знаходиться список розгорнутих додатків з найбільшим ризиком, включаючи кількість користувачів і рейтинг ризику, який створюється на основі комбінації рейтингів CTR, аналізу Cyberlab, категорії додатки і ризику області доступу.

Області доступу визначають, до яких даних додаток може отримати доступ у призначених для користувача середовищах, наприклад повні дані, контакти і можливість діяти від імені користувача. Визначення областей доступу може додати екстрені заходи захисту.

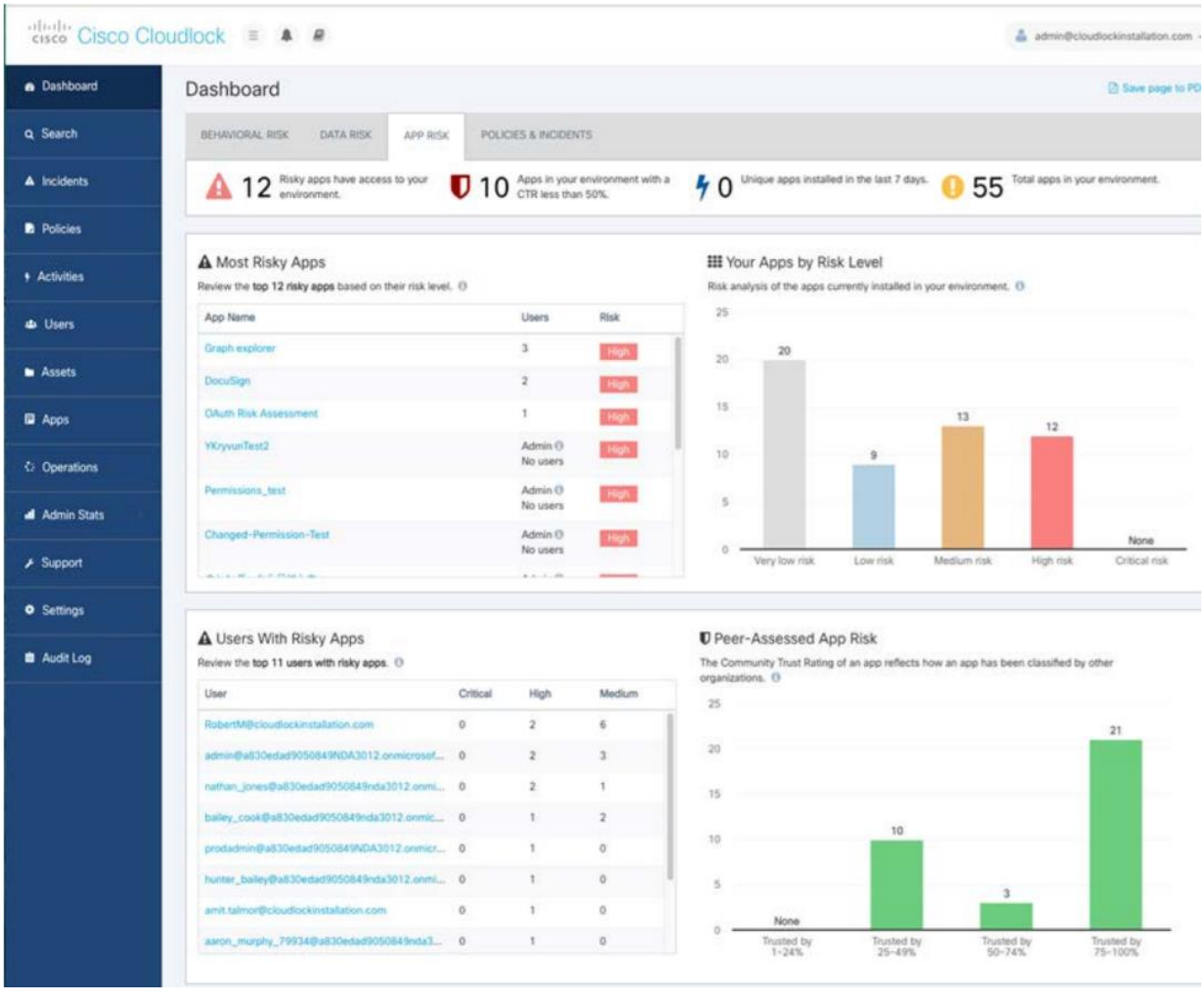
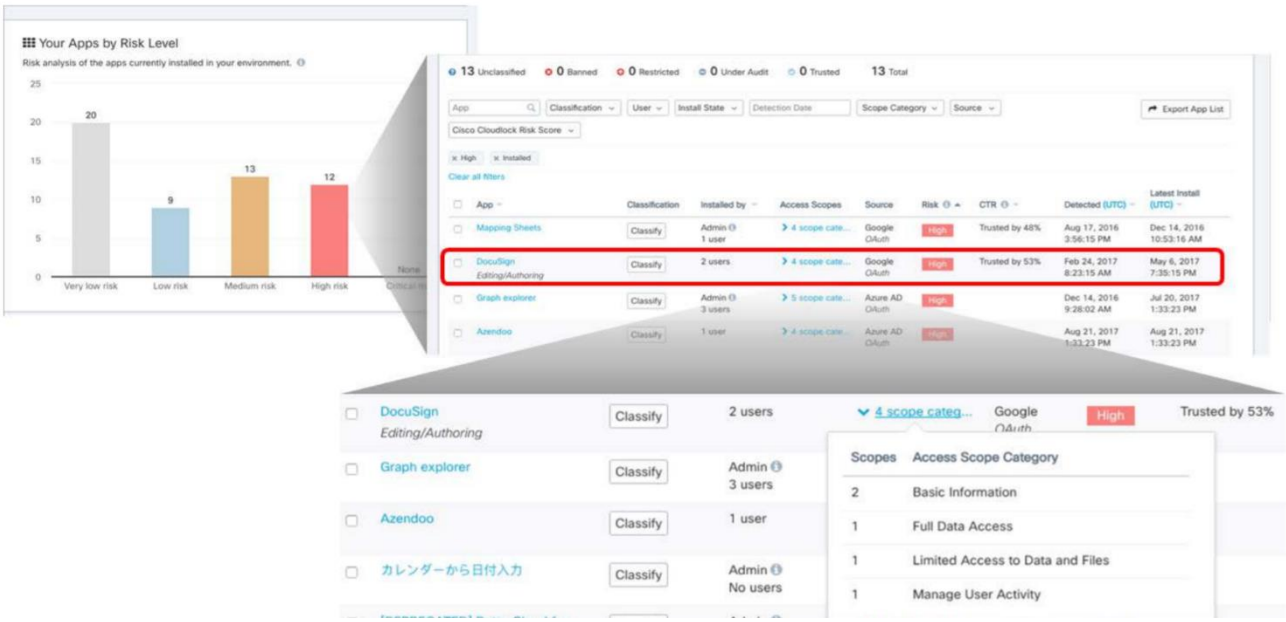


Рис. 2.13. Панель ризиків

Вгорі праворуч гістограма відстежує кількість додатків в кожній категорії ризику; при натисканні на панель високого ризику (нижче) відкриваються додаткові відомості про додатки з високим рівнем ризику за датою, а також відомості про кожного додатку, включеному в категорію. Клацання по назві додатка надає списки всіх подій додатки, користувачів і областей доступу, а

натискання на кнопку «Впорядкувати» дозволяє рекласифікувати додаток (рис. 2.14).

Адміністратори можуть легко і швидко побачити, до якої інформації має доступ кожен додаток, в стовпці Області доступу. Наприклад, ESG Lab переглянула області доступу DocuSign до додатка, підключеному до OAuth, включаючи доступ до основної інформації, повний доступ до даних, обмежений доступ до даних і



файлів, а також можливість управляти діями користувачів. Ці області доступу можуть викликати проблеми при зловмисному використанні, що є основною причиною того, що це додаток класифікується як додаток з високим ризиком.

Рис. 2.14. Інтерфейс функціоналу Cloudlock

Остання панель інструментів Policies & Incidents. У списку вказані всі хмарні платформи, а також оцінка безпеки і кількість користувачів цієї платформи; об'єкти; інциденти; критичні проблеми; оповіщення; та ін. Графік інцидентів за серйозністю можна фільтрувати по хмарної платформі; клацання по круговій діаграмі дозволяє адміністраторам переглядати інциденти, засновані на порушенні політики.

Коли ESG Lab клацала кругову діаграму, в новій виставі відображалися інциденти за політикам (див. Нижче). Було зареєстровано 23 інциденти, пов'язані з

політикою номерів соціального страхування, 12 - з політикою номерів кредитних карт і т. Д. Також доступний список користувачів з найбільшою кількістю інцидентів. Діаграма в правому верхньому кутку може відображати дані або за рівнем інциденту (критичний, попередження, попередження або інформація), або за ступенем дозволу. Всі інциденти перераховані внизу і можуть бути відсортовані за політику, статусу, платформі, власнику або серйозності. Показаний джерело інциденту, а також власники, статус інциденту і час виявлення.

Висновки до розділу 2

Отже, було проаналізовано методи та засоби забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock. Розглянуто призначення, основні функції та склад програмного комплексу Cisco Cloudlock. За рахунок сучасних алгоритмів, з’являється можливість на початку розпізнати аномалії поведінки та попередити можливу кібератаку.

Низка функцій, що пропонує Cisco Cloudlock є корисними та важливими для фахівців кібернетичної безпеки для забезпечення захисту хмарного середовища. Також було проаналізовано реалізацію технології забезпечення кібернетичної безпеки хмарного середовища в рішенні Cisco Cloudlock та закцентовано увагу на ключових її складових.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ РІШЕННЯ CISCO CLOUDLOCK

3.1. Варіант інтеграції технології кібербезпеки у хмару Dropbox Business на базі рішення Cisco Cloudlock

Варіант інтеграції технології кібербезпеки розроблений на реальному досліді впровадження системи захисту інформації у продуктовій компанії Boosta.co, що займається розробкою програмного забезпечення.

Cisco Cloudlock надає адміністраторам і групам безпеки поліпшену видимість і контроль в хмарних середовищах, що дозволяє швидко виявляти і реагувати на такі ризики, як кіберзагрози, спільне використання ресурсів і ненавмисне розкриття. Використовуючи хмарний підхід, Cisco Cloudlock додає додатковий рівень безпеки у середовище Dropbox вашої команди, відстежуючи активність облікових записів через Dropbox Business API.

Завдання Cisco Cloudlock:

1. Виявлення та розширення уявлення даних даних

Виявлення, якщо конфіденційна інформація, що зберігається в Dropbox, така як інтелектуальна власність, неправильно розкривається за допомогою налаштування механізму

2. Автоматизація реагування на інциденти

Карантин автоматично розкриває конфіденційну інформацію за допомогою дій реагування на основі політики Виявлення підозрілої діяльності при вході в систему Помітка незвичайної поведінки при аутентифікацій, що вказує на можливу компрометацію облікового запису, включаючи необмежені входи в систему і входи з різних геолокацій

3. Аналіз даних крос-платформ користувачів

Моніторинг поведінки користувачів у хмарних додатках для кореляції інформації.

Завдяки Cloudlock співробітники з відділу безпеки можуть краще відстежувати і контролювати події в своїй хмарної середовищі, швидко виявляти загрози (наприклад, кібер-загрози, порушення доступу, ненавмисне розкриття даних) і реагувати на них.

Cloudlock знижує ризики, пов'язані з витоком даних, тому що, відповідно до вказаної політикою автоматично додає файли в карантин, якщо виявляються засекречені відомості. Cloudlock використовує природний для хмари підхід і забезпечує додатковий рівень захисту вашої середовищі в Dropbox, відстежуючи діяльність облікового запису за допомогою різних API Dropbox Business.

3.2. Варіант технології забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock

Для інтеграції Cloudlock у хмару Dropbox Business необхідно відкрити дашборд та ознайомитися з розміщенням функціоналу (Рис. 3.1)

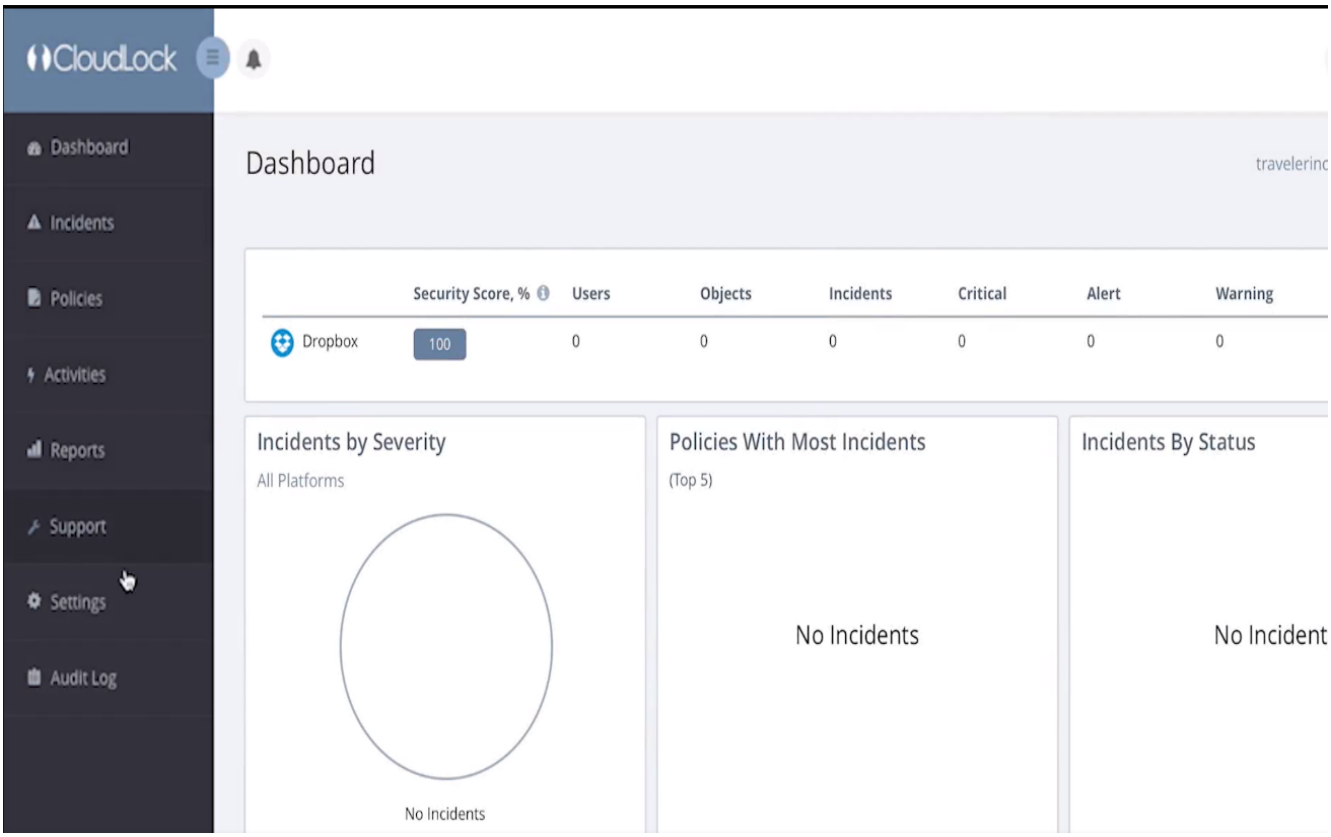


Рис. 3.1. Дашборд функціоналу

Далі необхідно пройти конфігурацію та обрати Dropbox як платформу (Рис. 3.2)

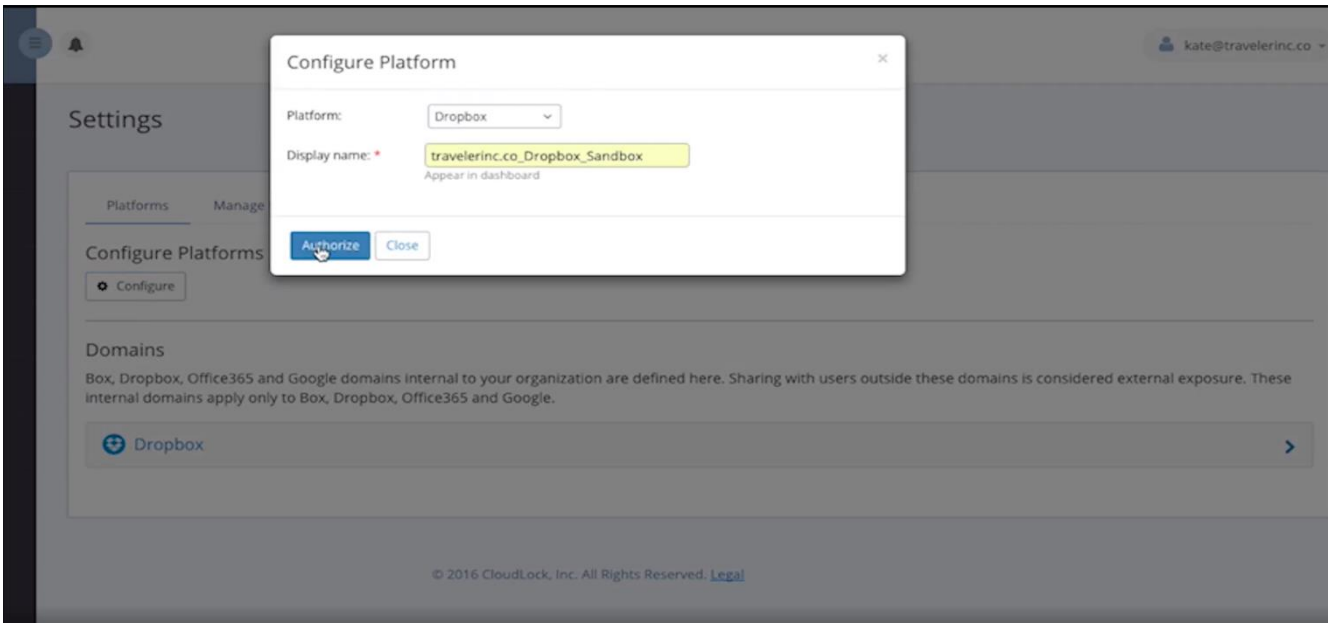


Рис. 3.2. Конфігурація платформи

Далі необхідно пройти авторизацію у Dropbox та надати доступ Cloudlock до даних (Рис. 3.3, Рис. 3.4)

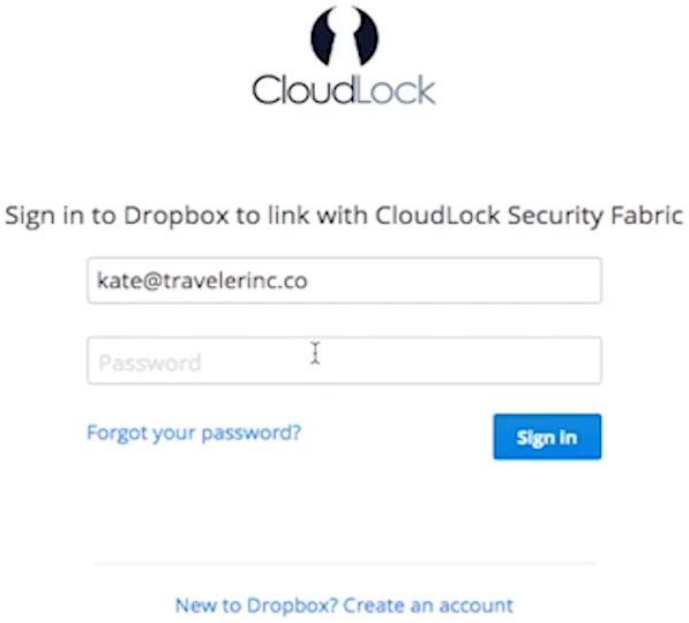


Рис. 3.3. Авторизація та вхід

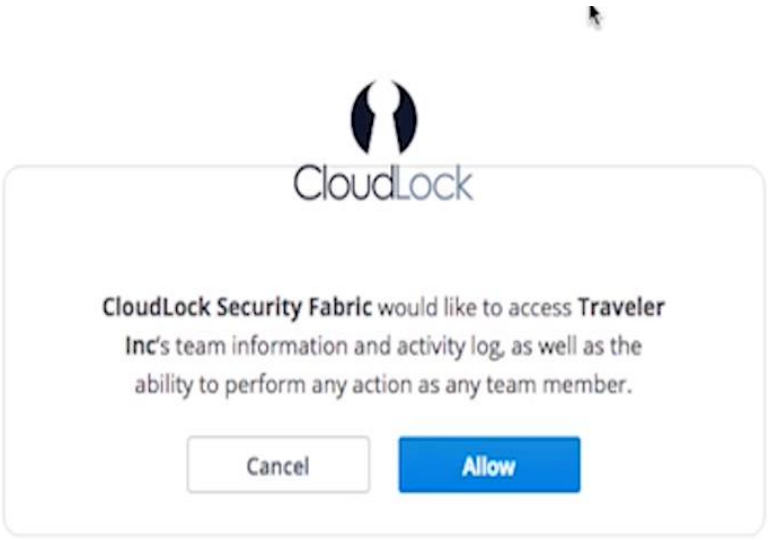


Рис. 3.4. Надання доступу Cisco Cloudlock

Також необхідно активувати існуючі політики (Рис. 3.5) або створити нові (Рис. 3.6, Рис. 3.7)

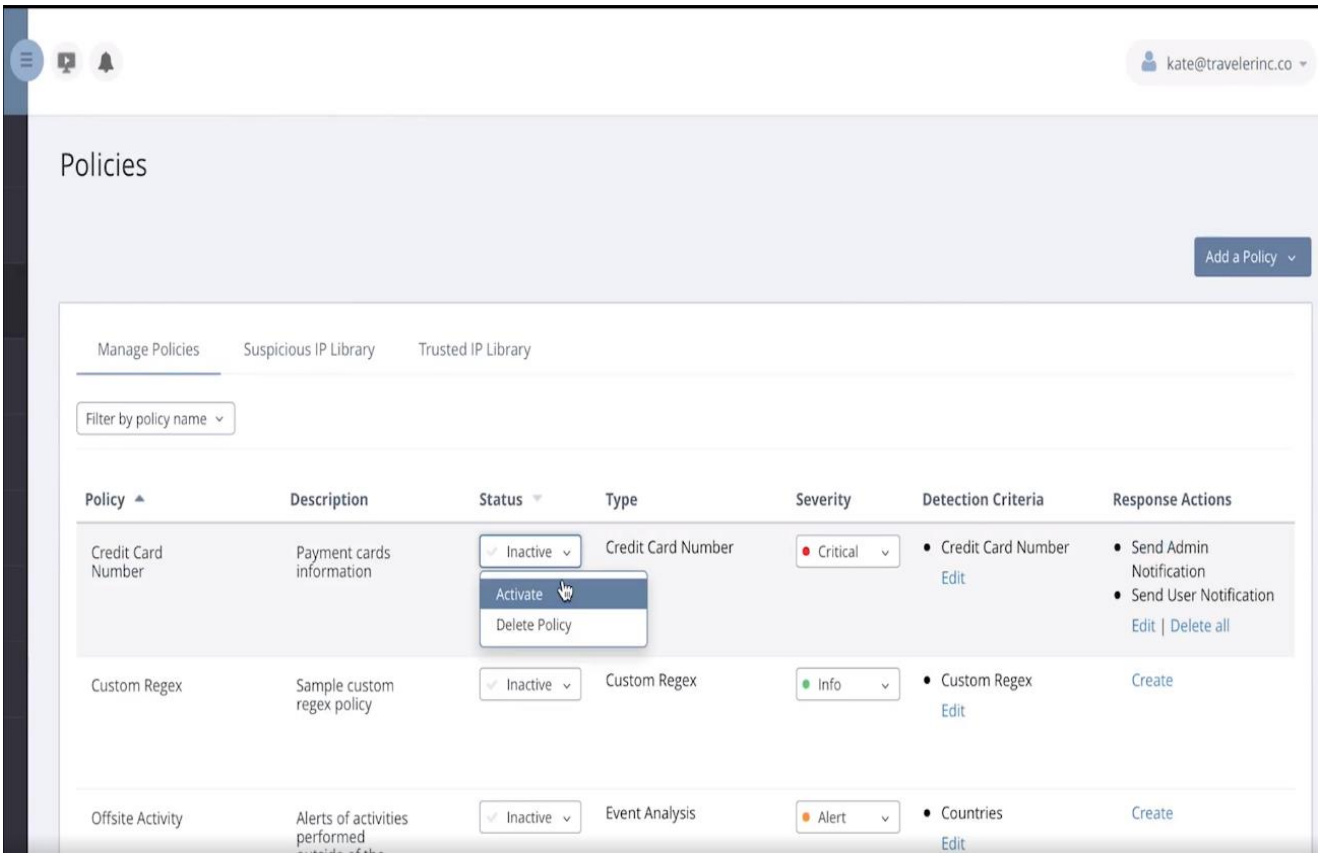


Рис. 3.5. Активація існуючих політик

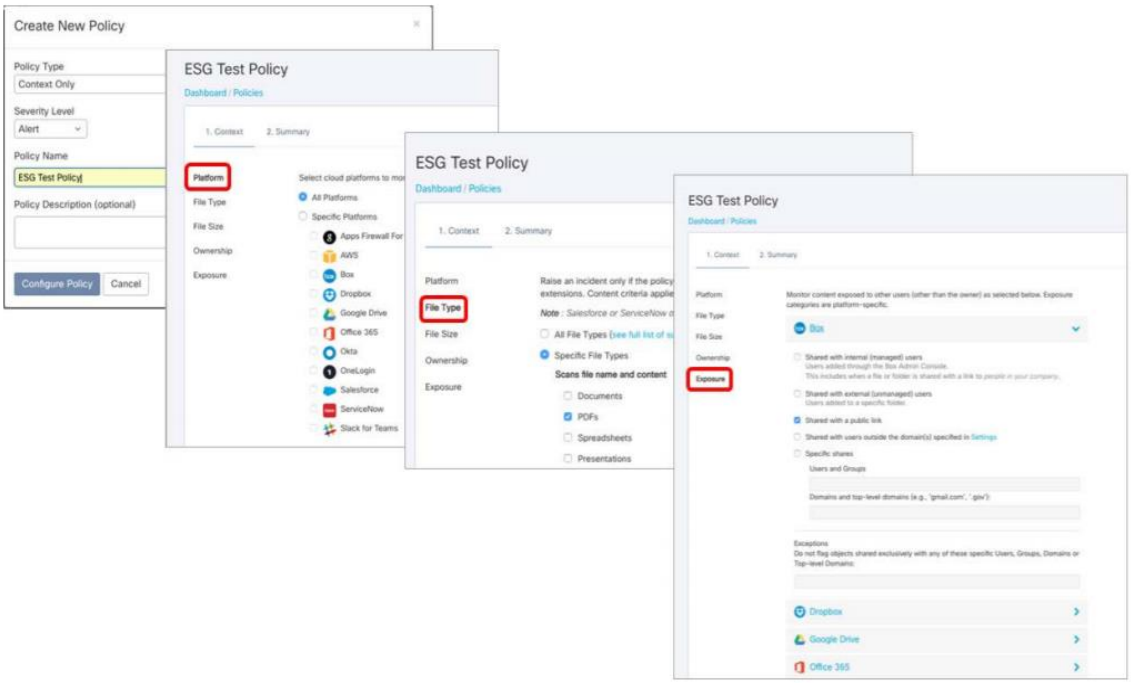


Рис. 3.6. Створення нової політики

Створення нової політики – фундамент та базова складова налагодженого функціонування Cisco Cloudlock. Тому є дуже важливим вказати всі параметри коректно та відповідно до загальним політикам компанії.

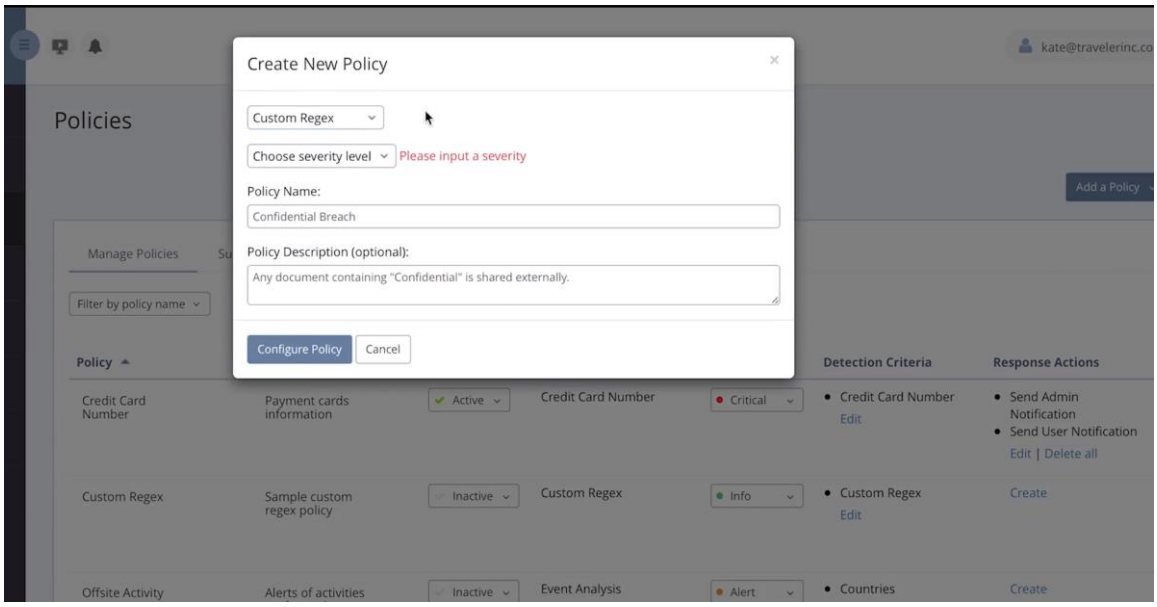


Рис. 3.7. Створення нової політики

Одне з головних складових успішного створення політики це додавання повної інформації у віконця опису (рис. 3.8, рис. 3.9)

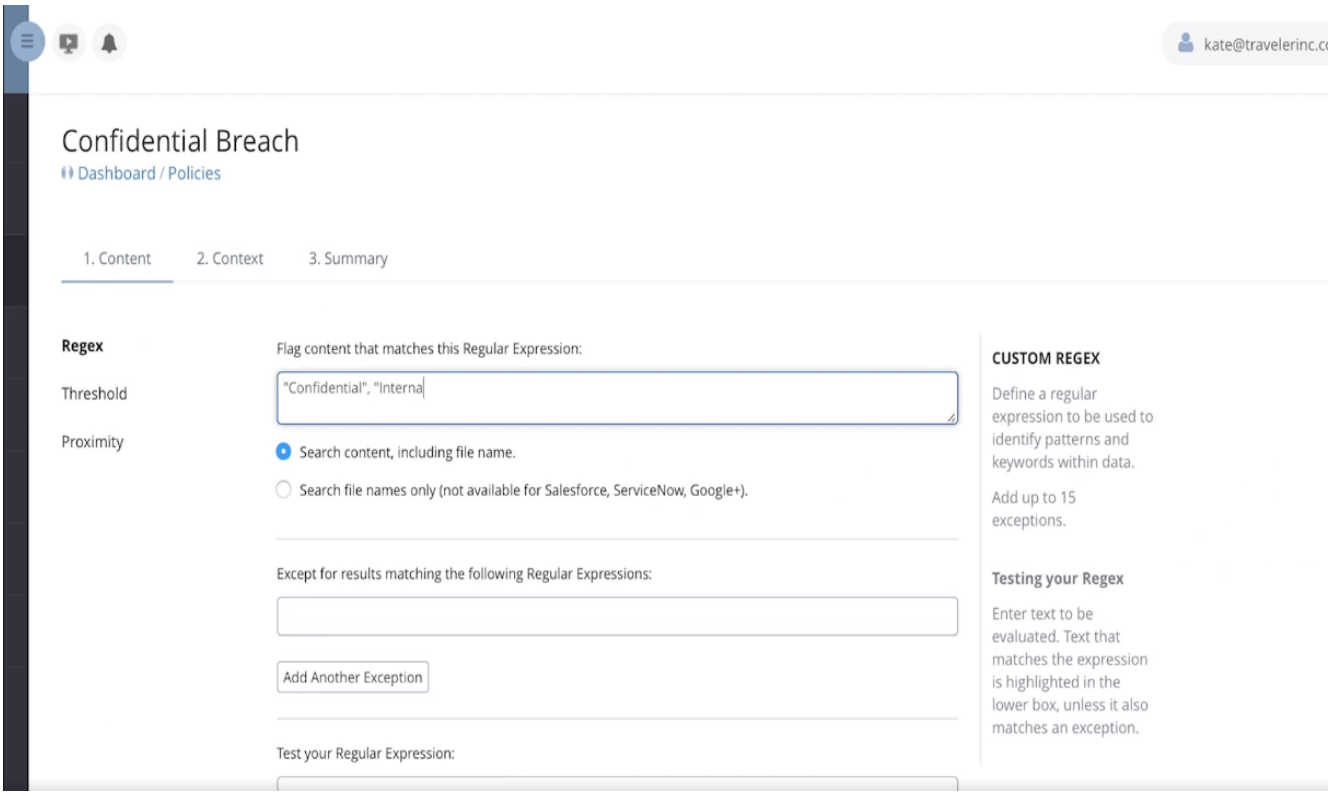


Рис. 3.8. Введення даних в описі правил

Введення даних в описі правила надають змогу цілісно зрозуміти функції кожної політики та уникнути помилок при інтеграції їх у хмару та початку роботи за даними.

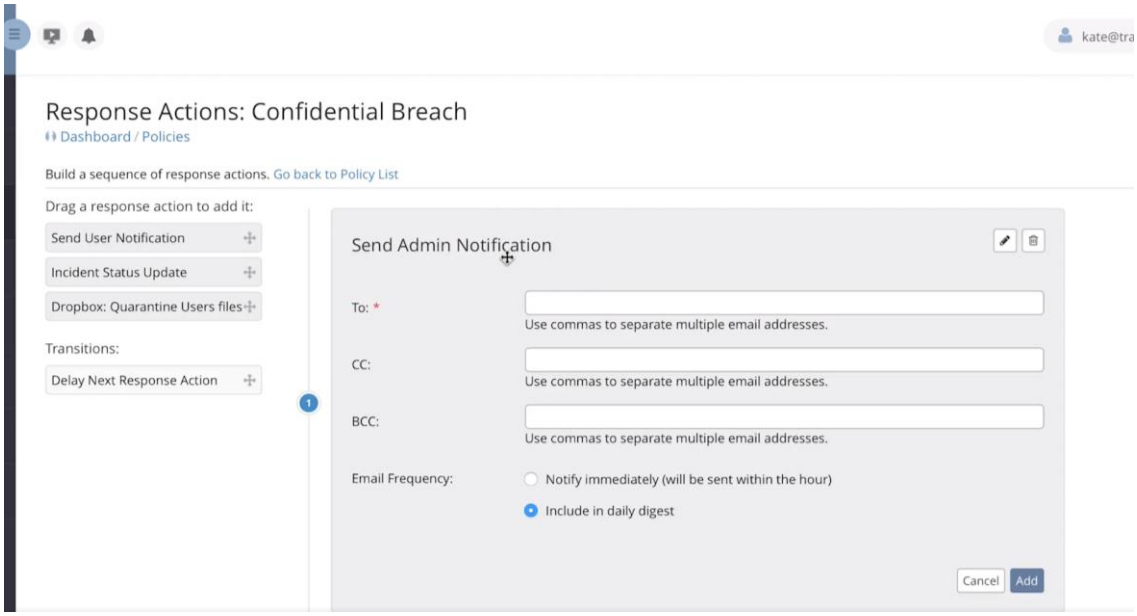


Рис. 3.9. Налаштування дій реагування

Після створення політик та повного налаштування функціоналу під потреби користувача, необхідно інтегрувати у Dropbox (рис. 3.10)

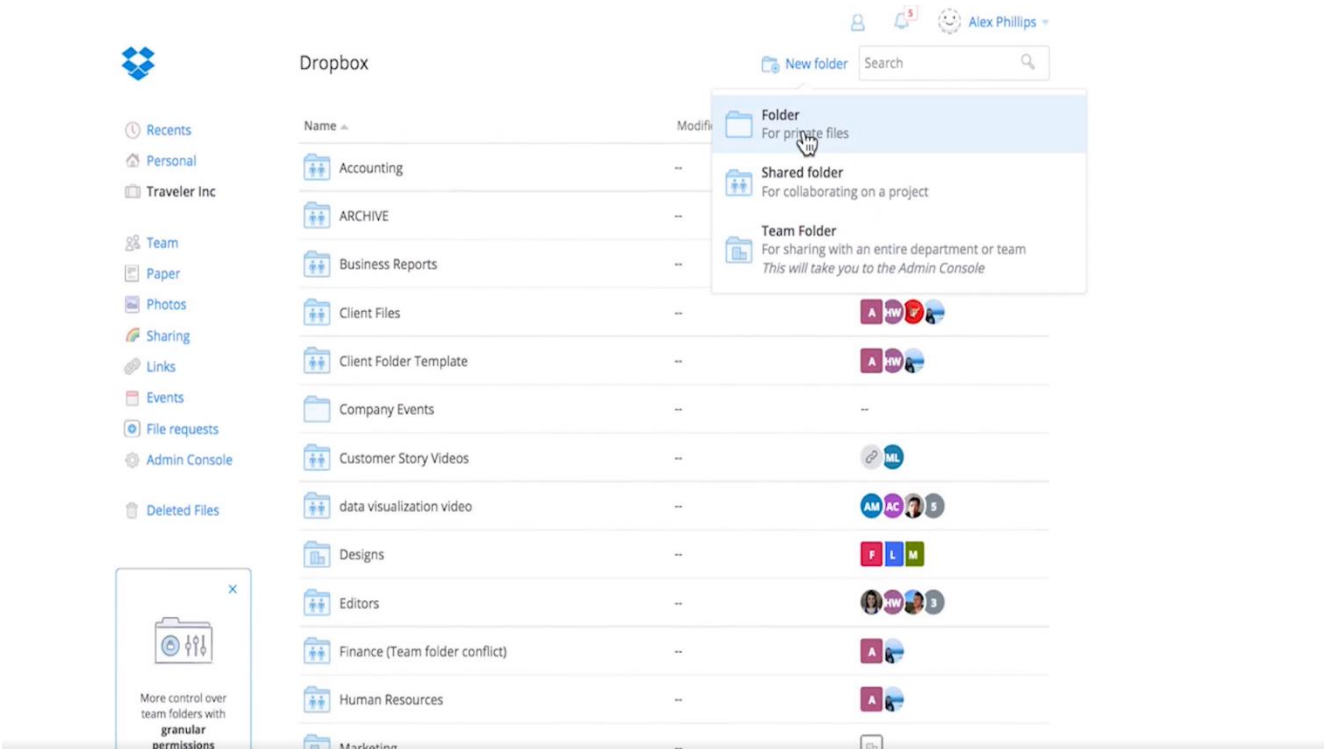


Рис. 3.10. Робота з Dropbox для інтеграції функціоналу Cisco Cloudlock

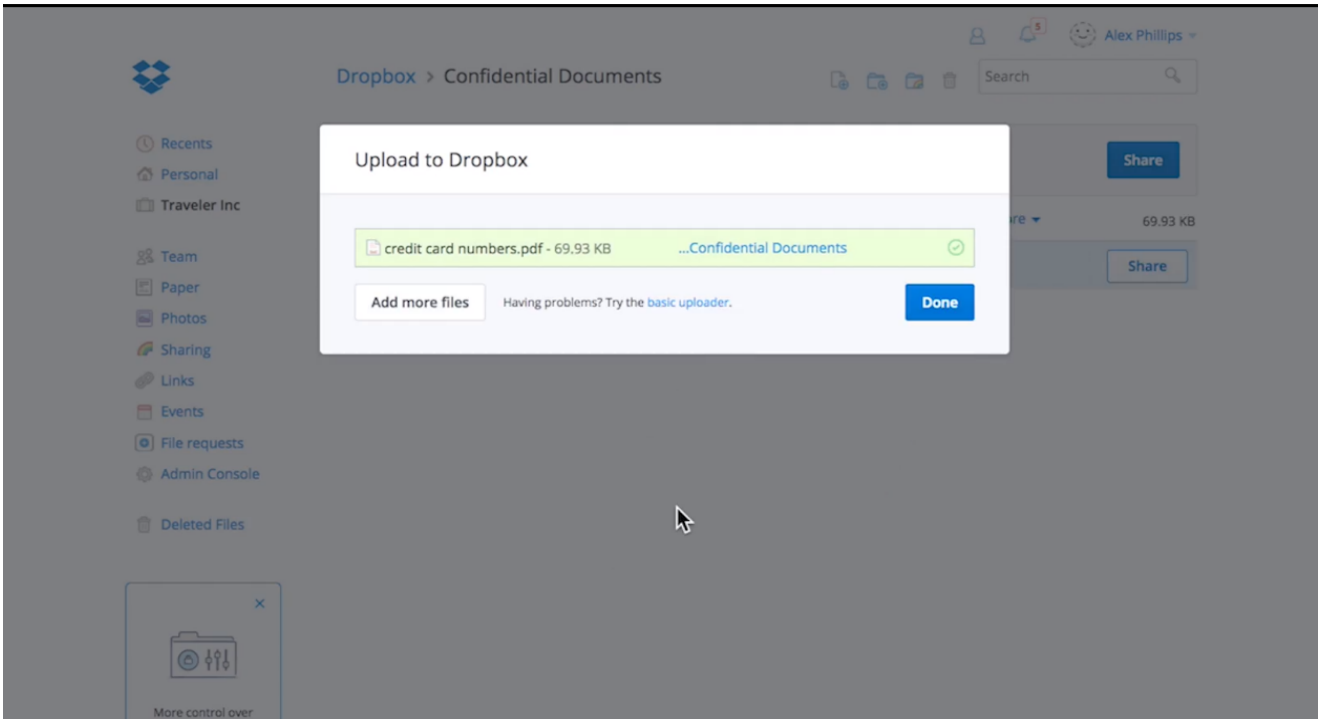


Рис. 3.11. Завантаження файлу у Dropbox для інтеграції функціоналу Cisco Cloudlock

В результаті буде отримано доступ до аналітики інцидентів та управління кібербезпеки у хмарному середовищі (рис. 3.12, рис. 3.13).

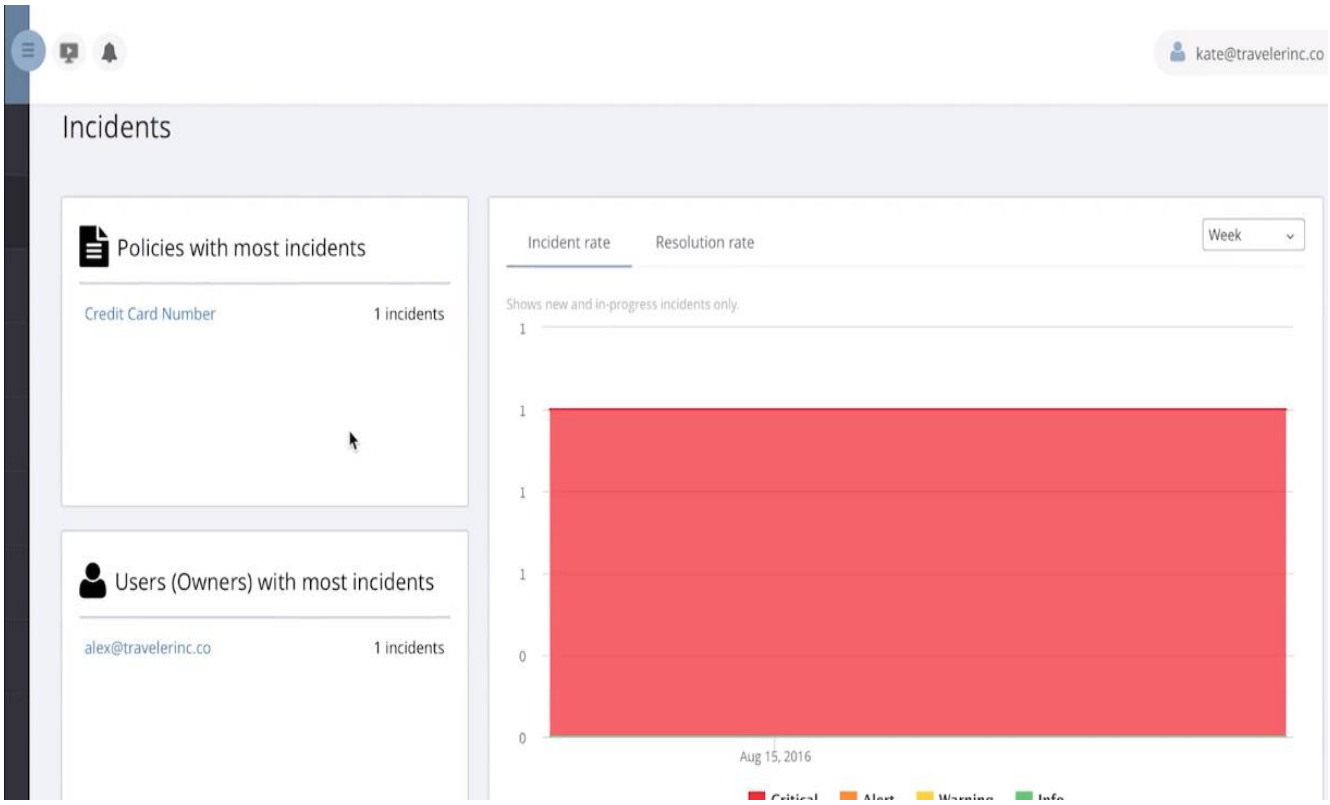


Рис. 3.12. Аналітика інцидентів

Аналітика інцидентів – ключ для успішного впровадження політик та налаштуванню. Завдяки цій функції є можливість бачити результати у реальному часі та виправляти помилки для постійного оновлення параметрів.

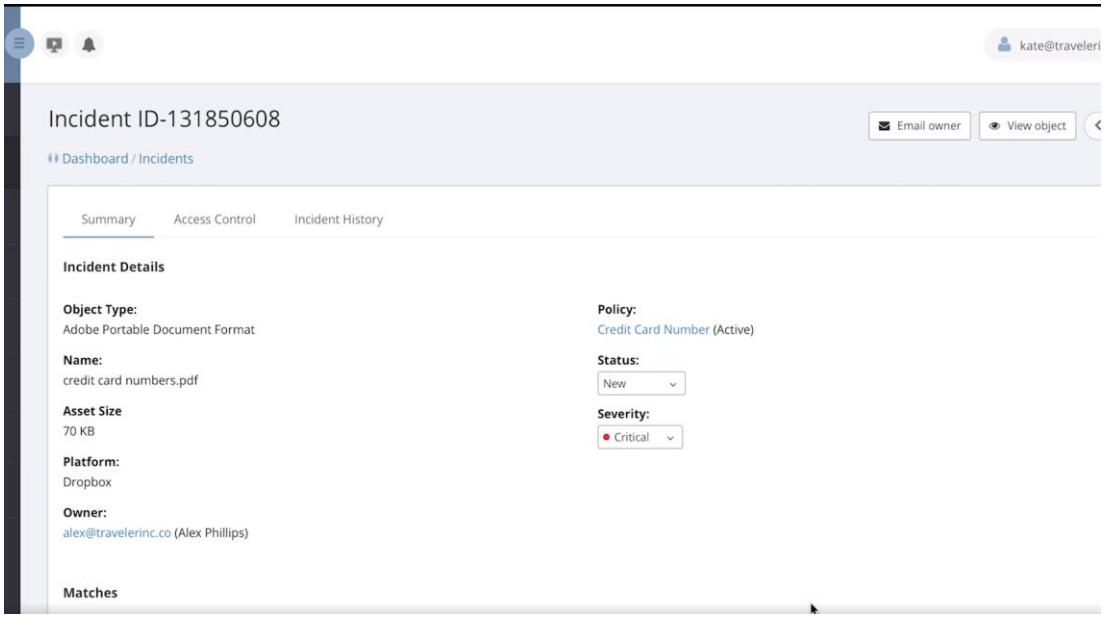


Рис. 3.13. Огляд окремо взятого інциденту

В результаті, отримано можливість забезпечення кібербезпеки у хмарному середовищі Dropbox Business. Така можливість існує і для хмари Dropbox для власних потреб.

Хмарний сервіс є особливою клієнт-серверною технологією, що передбачає використання користувачем ресурсів, таких як оперативна пам’ять, процесорний час, дисковий простір, мережеві канали, спеціалізовані контролери та інші, групи серверів у мережі, які між собою взаємодіють.

Для користувача вся група виглядає як єдиний віртуальний сервер. Користувач може прозоро та динамічно змінювати обсяги споживання даних ресурсів у випадку зміни необхідності, він може збільшувати, зменшувати потужність сервера з відповідною зміною оплати та інше. У такому випадку наявність кількох джерел ресурсів, що використовуються надає можливість підвищувати доступність системи клієнт-сервер за рахунок динамічного масштабування у випадку підвищення навантаження.

Також це знижує ризик припинення функціонування віртуального сервера під час виходу з ладу окремих серверів, що обслуговують клієнта, так як існує ймовірність автоматичного під’єднання віртуального сервера до ресурсів резервного сервера.

3.3. Розроблення рекомендацій щодо забезпечення кібербезпеки у хмарному середовищі

Для забезпечення кыбербезпеки у хмарному середовищі на базі рішення Cisco Cloudlock запропоновано правило та рекомаендації.

Відстеження і усунення витоку даних. За допомогою настроюваної політики устаткування можна відстежувати, випадки надання не належного доступу до важливих даних в Dropbox (наприклад, до об'єктів права інтелектуальної власності та PCI).

Автоматична реакція на події. За допомогою встановленої в політиці реагування на події можна автоматично додавати в карантин, щоб не піддаювати ризику важливі дані.

Відстеження підозрілих входів в обліковий запис. Можна відзначати нехарактерні пов'язані з аутентифікацією події, які можуть означати несанкціонований доступ до аккаунту (в тому числі дивні входи в систему і веб-сеанси, вироблені з незвичайних географічних точок).

Відстеження дій на різних платформах. Можна аналізувати дані про поведінку користувачів в різних хмарних додатках (в тому числі SaaS, IaaS, PaaS і IDaaS), щоб отримати взаємопов'язані і всебічні висновки про безпеку.

Cisco Web Security Appliance

Можливо зробити так, щоб організації обмежили використання неавторизованих особистих акаунтів Dropbox в корпоративних мережах, і в той же час дозволити доступ до керованим компанією акаунтів за допомогою Cisco Web Security Appliance і мережевого контролю Dropbox.

Розширення захист від регульованих програм (AMP) - це додатково ліцензійна функція, доступна всім клієнтам Cisco WSA. AMP - це комплексне рішення для захисту від небезпечних програм, що забезпечує виявлення та блокування шкідливих програм, неперервний аналіз та ретроспективні попередження. Він використовує переваги захищених інтелектуальних мереж обласної безпеки як Cisco, так і Sourcefire (тепер частина Cisco).

AMP доповнює можливості виявлення та блокування врегульованих програм, запропонованих у Cisco WSA, з розширеними можливостями репутації файлів, детальними повідомленнями про передачу файлів, неперервним аналізом файлів та ретроспективним попередженням.

У клієнтів є можливість виділити файли PDF та Microsoft Office у доповненні до файлів EXE, підтримуючи їх у першій версії AMP. Монітор трафіка рівня 4 постійно сканує активність, виявляючи та блокуючи зв'язок «телефон-будинок» шпіонського ПО. Завдяки всім додатковим додаткам, Layer 4 Traffic Monitor ефективно залишає за собою врегульоване ПО, яке намагається знайти класичні рішення веб-безпеки. Він динамічно надає IP-адресу відомих вредоносних доменів у вашому списку тимчасових об'єктів для блокування.

Cisco WSAV пропонує всі ті функції, що і Cisco WSA, з додатковим зручністю та економією засобів моделей віртуального розгортання, включаючи незадовільне самообслуговування. З ліцензією Cisco WSAV підприємства можуть розробити віртуальні шлюзи веб-безпеки без підключення до Інтернету, застосовуючи ліцензію на новий файл віртуального утворення Cisco WSAV, хранящемуся локально.

За необхідності файлів оригінального віртуального узагальнення можна клонувати для немедленного розвертання декількох шлюзів веб-безпеки. Запустіть обладнання та віртуальні машини в одній розробці. Невеликі філіали або удалені місцяположення можуть мати таку же захист, що забезпечує Cisco WSA, без необхідності встановлення та підтримки обладнання в цьому місці. Настраиваемым развертыванием легко управляти за допомогою Cisco Content Security Appliance Management.

Підхід до єдиного продукту пішов в минуле. Це було б недостатньо та неефективно для боротьби з кіберзагрозами. Протягом останніх кількох років був впроваджений архітектурний підхід для забезпечення наскрізної безпеки.

Cisco об'єднує всю інформацію, зібрану за допомогою різних протоколів і додатків, включаючи систему доменних імен (DNS), Інтернет (HTTP і HTTPS), FTP, електронну пошту (простий протокол передачі пошти) і простий протокол управління мережею, серед іншого, в Talos ™ (Cisco розвідка загроз). У цьому документі ми інтегруємо Cisco Umbrella з WSA для забезпечення безпеки на декількох рівнях з використанням DNS і веб-трафіку.

Cisco Umbrella - це платформа хмарної безпеки, яка забезпечує перший рівень захисту від загроз для всіх додатків. DNS є основною вимогою для підключення до Інтернету, і він забезпечує широку видимість для різних кінцевих точок, від серверів, робочих станцій і ноутбуків, мобільних телефонів, а також керованих і некерованих пристроїв до пристроїв Інтернету речей (IoT).

WSA - це рішення веб-проксі, яке ще більше підвищує безпеку, пропонуючи деталізовані елементи управління веб-використанням, включаючи видимість і контроль додатків (AVC), а також настроюються заголовки для відповідності.

WSA виконує глибоку перевірку пакетів для всього веб-трафіку, будь то простий текст або зашифрований. Інтеграція між обома продуктами допоможе забезпечити повний захист організацій.

Ця інтеграція допоможе прикрити атаки з боку відомих хороших доменів, на яких містить шкідливі програми (WSA), і недавно виявлених доменів, де Cisco Umbrella має краще покриття. Це також допоможе розшифрувати весь трафік Secure Sockets Layer, щоб гарантувати відсутність прихованих шкідливих програм (WSA) і, що найбільш важливо, забезпечити видимість різних векторів атак - не тільки через DNS або Інтернет, а й через інші протоколи, які підтримуються Talos Intelligence.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення захисту хмарного середовища як складової частини корпоративної інформаційної системи, встановлена сутність завдань їх захисту.

Проаналізовано існуючі технології захисту хмарного середовища. Досліджена технологія управління кібербезпекою хмарного середовища на прикладі рішень Cisco Cloudlock.

Визначено методи та засоби забезпечення управління кібербезпекою хмарного середовища на базі рішень Cisco Cloudlock.

Встановлено основні функції та принципи роботи програмного комплексу Cisco Cloudlock – це програмне забезпечення, яке призначене для захисту хмарного середовища від новітніх загроз. Також воно допомагає адміністраторам безпеки забезпечувати відповідність хмарного середовища політикам безпеки.

Встановлено основні функції та принципи роботи програмного комплексу Cisco Cloudlock. Cisco Cloudlock - спеціальне рішення для хмари для безпечного доступу до такого середовища. Брокер дозволяє безпечно проводити операції в хмарі. Cisco Cloudlock націлений на захист користувачів, даних і додатків в хмарі. Надає можливість створити колективний рейтинг довіри для додатків і внесення їх в білий або чорний список в залежності від рівня потенційного ризику.

Cisco Cloudlock забезпечує крос-платформне аналітику поведінки користувачів та суб'єктів (UEBA) для SaaS, середовища IaaS, PaaS та IDaaS. Cisco Cloudlock використовує вдосконалене машинне навчання, алгоритми виявлення аномалій на основі таких факторів, як діяльність поза білим списком країни та дії на відстані з неможливою швидкістю.

Cisco Cloudlock - це захист від потенційної небезпеки хмарного доступу (CASB). Cisco Cloudlock захищає хмарні ідентифікатори, дані та додатки, забезпечує відповідність вимогам політики безпеки та підвищує ефективність. Cisco Cloudlock - це відкрите та автоматизоване рішення, яке створюється з

урахуванням хмарних навчальних записів, використання даних та ризиків екосистеми програм, що надає діючі аналітичні дані про кібербезпеку.

У роботі запропоновано варіант забезпечення кібернетичної безпеки хмарного середовища на базі Cisco Cloudlock.

Для виконання цих завдань програмне забезпечення Cisco Cloudlock має встановлюватися на кожній окремій хмарі. У хмарному середовищі, тобто інформаційній системі налаштовуються функції та політики, здійснюється керування ними за допомогою комплексу Cisco Cloudlock.

Розроблено рекомендації фахівцям кібернетичної безпеки щодо застосування технології захисту хмарного середовищі у корпоративному сегменті.

Таким чином, правильна реалізація технології захисту хмарного середовища на базі рішень Cisco Cloudlock має забезпечити ефективний захист та кібербезпеку хмарного середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gartner. Magic Quadrant for Unified Endpoint Management Tools. 6 August 2019. Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith [Електронний ресурс] – Режим доступу: https://www.gartner.com/doc/reprints?id=1-1ODRVFHP&ct=190812&st=sb.

2. Committee on National Security Systems (CNSS). Glossary. CNSSI No. 4009. April 6, 2015 [Електронний ресурс] – Режим доступу: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

3. Василенко В. В. Реконфігурації моделі мережі для масштабованості SDN / В. В. Василенко // Наукові записки УНДІЗ. – 2016. – №3 (43) – С. 62 – 71.

4. Василенко В.В. SDN як платформа підвищення безпеки в телекомунікаційних мережах / Гринкевич Г.О., Куклов В.М., Василенко В.В. // матеріали науково-технічної конференції студентів, аспірантів, викладачів та науковців: 18 грудня 2014 року. – К. : Державний університет телекомунікацій, – 2014. – 111 с.

5. Василенко В.В. Аналіз світового досвіду підвищення прибутків провайдерів за рахунок реалізації технології SDN / В. М. Куклов, В. В. Василенко : міжнародна науково-технічна конференція [Сучасні інформаційнотелекомунікаційні технології],(Київ,17-20 листопада 2015 р.) – К. : Державний університет телекомунікацій, 2015. – С. 137 – 138.

6. Василенко В.В. Використання SDN для аналітичної моделі графа атак / Василенко В. В. : восьма міжнародна науково-технічна конференція [Проблеми інформатизації], (Київ, 11-12 квітня 2017 р.) – К. : Державний університет телекомунікацій, 2017. – С. 29 – 30.

7. Василенко В.В. Масштабованість SDN на основі реконфігурації моделі мережі з урахуванням безпеки і QOS обмежень / В. В. Василенко // Сучасний захист інформації 2016. – №3, – С. 48 – 55.

8. Василенко В.В. Оцінка навантаження інфокомунікаційної мережі / Коршун Н.В., Гринкевич Г.О., Василенко В.В. та ін. // Системи управління, навігації та зв’язку. Випуск 1 (33). – Полтава, 2015. – С. 107 – 110.

9. Василенко В.В. Технологія SDN в сучасних телекомунікаційних мережах / В. В. Василенко, І. І. Бондаренко : матеріали першої міжнародної науково-технічної конференції [Актуальні проблеми розвитку науки і техніки:], (Київ 22 жовтня 2015 року). — К. : ДУТ, 2015. Збірник тез. – 189 с.

10. Вишнівський В. В. Схема контролю технічного стану цифрових блоків безконтактним індукційним методом / Вишнівський В. В., Кузавков В. В., Василенко В. В. // Зв'язок. – 2014. – (№4). – С. 28 – 32.

11. V. Vasylenko Analysis of SDN for wireless handover platform / V. Vasylenko, V. Kuklov, G. Grynkevych : матеріали International Conference on (Modern Problems of Radio Engineering) // Telecommunications and Computer Science (TCSET) – 2016 – 13th. – Lviv : 2016, pp. 630 – 633. doi: 10.1109/TCSET. – 2016.7452136. [Електронний ресурс] – Режим доступу : http://ieeexplore.ieee.org/document/7452136/?reload=true.

12. International Working Group on Data Protection in Telecommunications (IWGDPT) [Електронний ресурс]. - Режим доступу : http://clck.ru/8aXVe

13. Working Paper on Cloud Computing - Privacy and data protection issues (“Sopot Memorandum”). International Working Group on Data Protection in Telecommunications 51st meeting, 23-24 April 2012, Sopot (Poland) [Електронний ресурс]. - Режим доступу : http://clck.ru/8aJ9c

14. Мошеннические облачные сервисы - бич 77% компаний. SecurityLab.ru. 23.01.13. [Електронний ресурс]. - Режим доступу : http://www.securitylab.ru/news/436587.php

15. Firms Run Data Protection Risk by Not Checking Where Information is Held in the Cloud. Icomm Technologies. 05.11.2012 [Електронний ресурс]. - Режим доступу: http://www.icomm.co.uk/Thought-Leadership/Press-Releases/Firms-Run-Data…; Облачные провайдеры прячут данные от заказчиков [Електронний ресурс]. - Режим доступу: http://www.cnews.ru/news/top/index.shtml?2012/11/21/510449

16. IT-специалисты не спешат доверить свои данные "облаку". NEWS.ru.com. Технологии. 14.12.2012. [Електронний ресурс]. - Режим доступу: http://hitech.newsru.com/article/14dec2012/cloudrisk

17. Lieberman Software: IT-специалисты не доверяют облачным сервисам. SecurityLab.ru. 14.12.2012. [Електронний ресурс]. - Режим доступу: http://www.securitylab.ru/news/435160.php

18. U.S. Companies View Cloud Computing as Key to Improved Data Protection [Електронний ресурс]. - Режим доступу: http://investor.ca.com/releasedetail.cfm?releaseid=674043

19. Cloud Computing. Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA). November, 2009. [Електронний ресурс]. - Режим доступу: http://www.enisa.europa.eu/activities/risk-management/files/deliverable…

20. Commission proposes a comprehensive reform of the data protection rules. Правовий портал Європейської Комісії. [Електронний ресурс]. - Режим доступу: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

21. Див. наприклад: Working Paper on Cloud Computing Privacy and Data Protection Issues (“Sopot Memorandum”). / International Working Group on Data Protection in Telecommunications. 51st meeting, 23-24 April 2012, Sopot (Poland) [Електронний ресурс]. - Режим доступу: http://www.datenschutz-berlin.de/content/europa-international/internati…;

22. Dr Giles Hogben. ENISA Cloud Computing Security Strategy / European Network and Information Security Agency (ENISA). 2012. [Електронний ресурс]. - Режим доступу: http://www.enisa.europa.eu/.

23. Unleashing the Potential of Cloud Computing in Europe. European Commission/ Brussels, 27.9.2012COM(2012) 529 final [Електронний ресурс]. - Режим доступу: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/…

24. Digital Agenda: New strategy to drive European business and government productivity via cloud computing [Електронний ресурс]. - Режим доступу: http://europa.eu/rapid/press-release_IP-12-1025_en.htm?locale=en

25. European Commission. Unleashing the Potential of Cloud Computing in Europe – What is it and what does it mean for me? Memo. [Електронний ресурс]. - Режим доступу : http://www.abbl.lu/sites/abbl.lu/files/FAQ_Cloud_Computing.pdf

26. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. September 2011. [Електронний ресурс]. - Режим доступу : http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf;

27. Облачные вычисления. Материал из Википедии — свободной энциклопедии [Електронний ресурс]. - Режим доступу : http://clck.ru/8aIuk;

28. Cloud computing. From Wikipedia, the free encyclopedia [Електронний ресурс]. - Режим доступу: http://en.wikipedia.org/wiki/Cloud_computing

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

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

Магістерська робота
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ РІШЕННЯ CISCO CLOUDLOCK»

Виконав: МІСЕВІЧ Катерина Сергіївна

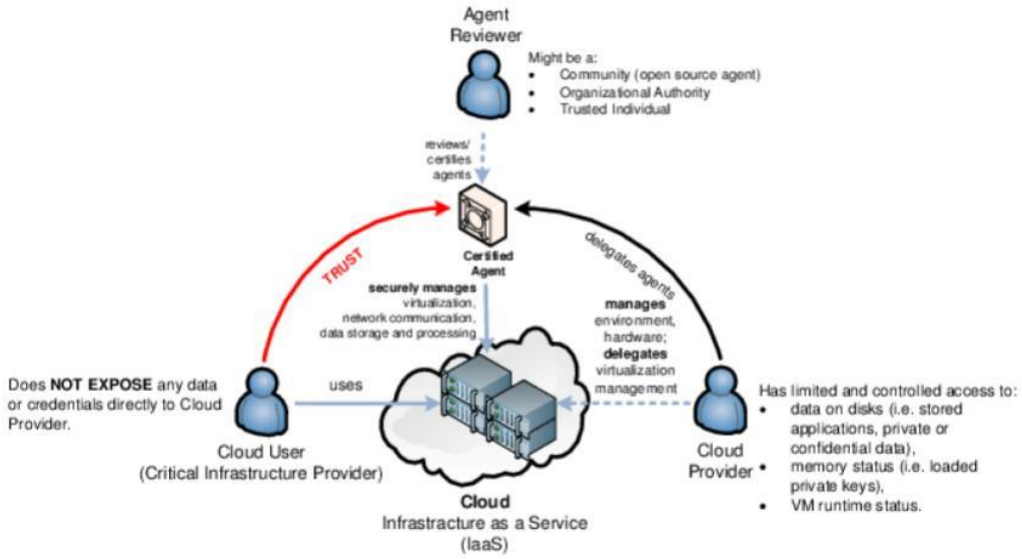
Керівник: к.військ.н. ГАХОВ Сергій Олександрович

3

Хмари - це великий ресурс простих у використанні та доступних віртуалізованих сервісів (наприклад апаратні засоби, платформи розробки, послуги та інше).

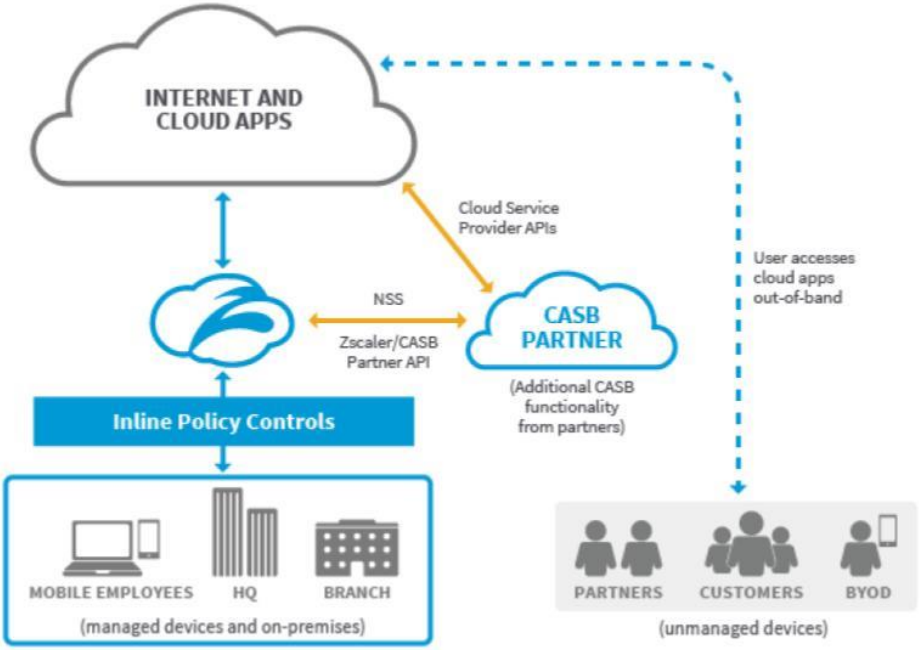
Ці ресурси зазвичай динамічно реконфігуровані, для того, щоб пристосуватися до нестабільного навантаження, що також дозволяє ефективно використовувати ресурси.

Проблеми у забезпеченні кібербезпеки хмарного середовища

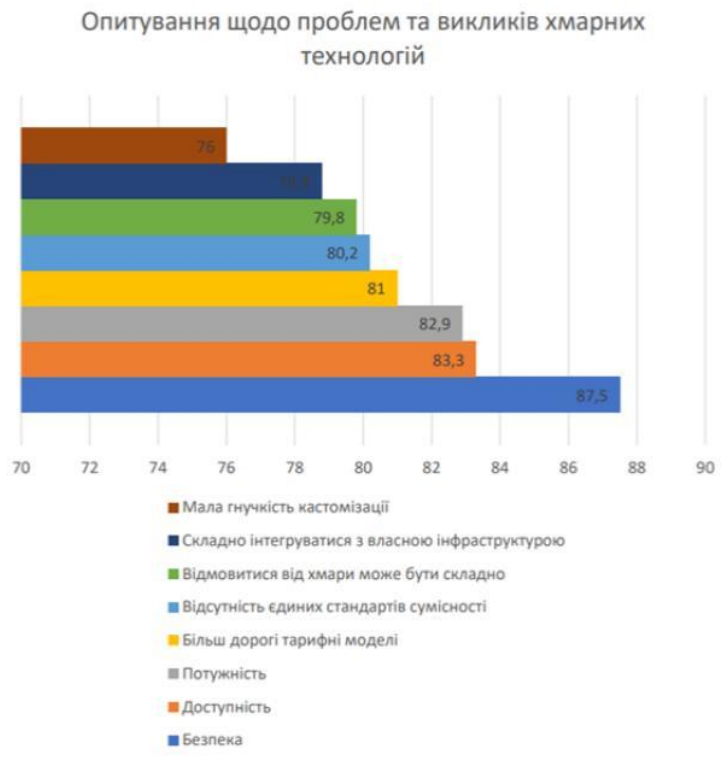


4

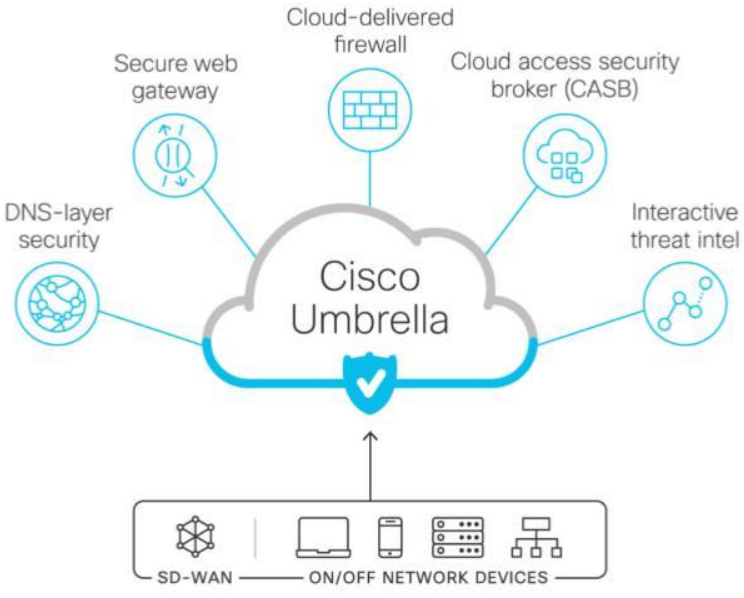
Cloud Access Security Broker (CASB) - це технологія контролю та безпеки, яка розташовується між cloud клієнтом і cloud провайдером.



5

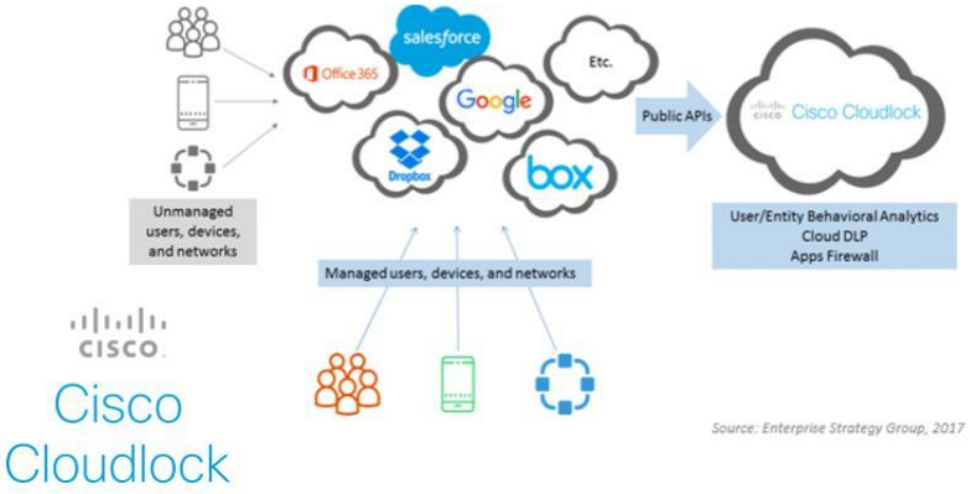


Компанія Cisco Systems, визнаний лідер в області мережевих рішень, пропонує також широкий вибір продуктів в області забезпечення інформаційної безпеки



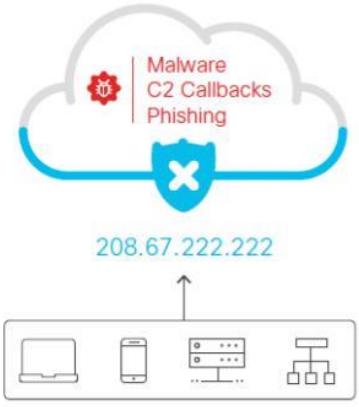
Cisco Cloudlock пропонує рішення брокера безпеки доступу до хмарної середовищі (CASB), що допомагають організаціям використовувати хмару безпечним чином. забезпечуючи наочність і контроль користувачів, даних і додатків для середовищ «програмне забезпечення як послуга» (SaaS), «платформа як послуга »(PaaS) і« інфраструктура як послуга »(IaaS)

. Також компанія забезпечує корисний аналіз кібербезпеки завдяки власним центру CyberLab з фахівцями, а також аналіз безпеки за принципом краудсорсингу.



CISCO

Cisco Cloudlock



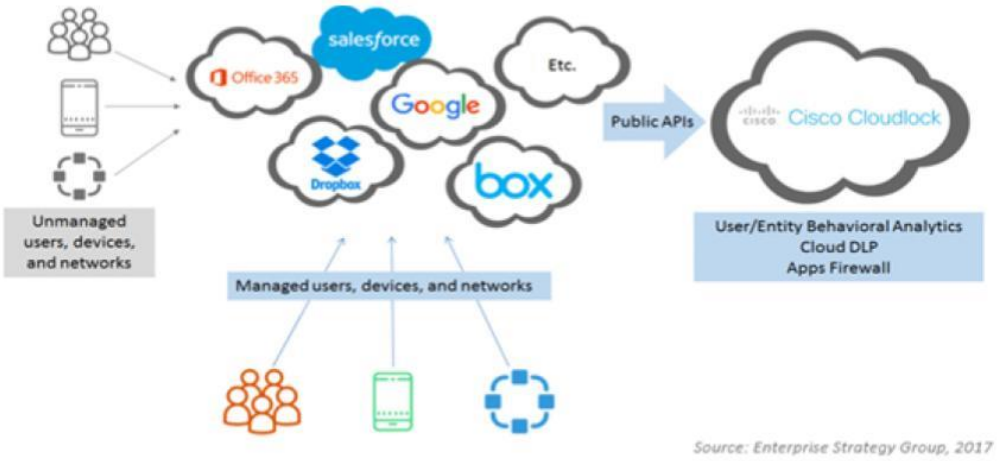
Типові рішення платформи Cloudlock CASB безпеки працюють шляхом захисту периметра мережі, захисту трафіку в мережі і управління мобільні пристрої.

Ключові функції Cisco Cloudlock:

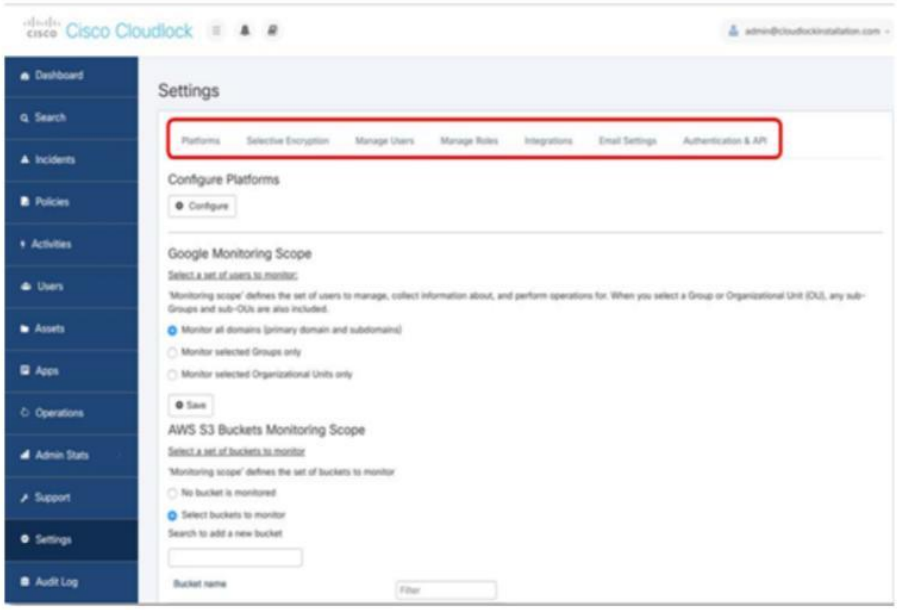
1. Аналіз поведінки користувачів та організацій
2. Право застосування на основі політики
3. Захист від загроз

В результаті дії Cloudlock не впливають на продуктивність або масштабованість так само, як проксі або шлюзи. Cloudlock налаштовується швидко і легко, не відволікаючи користувачів.

Cisco Cloudlock забезпечує крос-платформне аналітику поведінки користувачів та суб'єктів (UEBA) для SaaS, середовища IaaS, PaaS та IDaaS. Cisco Cloudlock використовує вдосконалене машинне навчання, алгоритми виявлення аномалій на основі таких факторів, як діяльність поза білим списком, списком країн та дії на відстані з не допустимою швидкістю та інше.



Налаштування Cloudlock відбувається в рамках вже розгорнутого середовища Cloudlock. На вкладці «Налаштування» ESG Lab можна легко управляти платформами, шифрувати файли, додавати і видаляти користувачів і ролі, управляти інтеграцією з іншими додатками, такими як безпека Cisco Umbrella DNS, а також керувати логінами SSO і токенами API.



11

Рекомендацій щодо застосування технології захисту корпоративних комп’ютерів на підприємстві

Відстеження і усунення витоку даних. За допомогою настроюваної політики устаткування можна відстежувати, випадки надання не належного доступу до важливих даних в Dropbox (наприклад, до об'єктів права інтелектуальної власності та PCI).

Автоматична реакція на події. За допомогою встановленої в політиці реагування на події можна автоматично додавати в карантин, щоб не піддаювати ризику важливі дані.

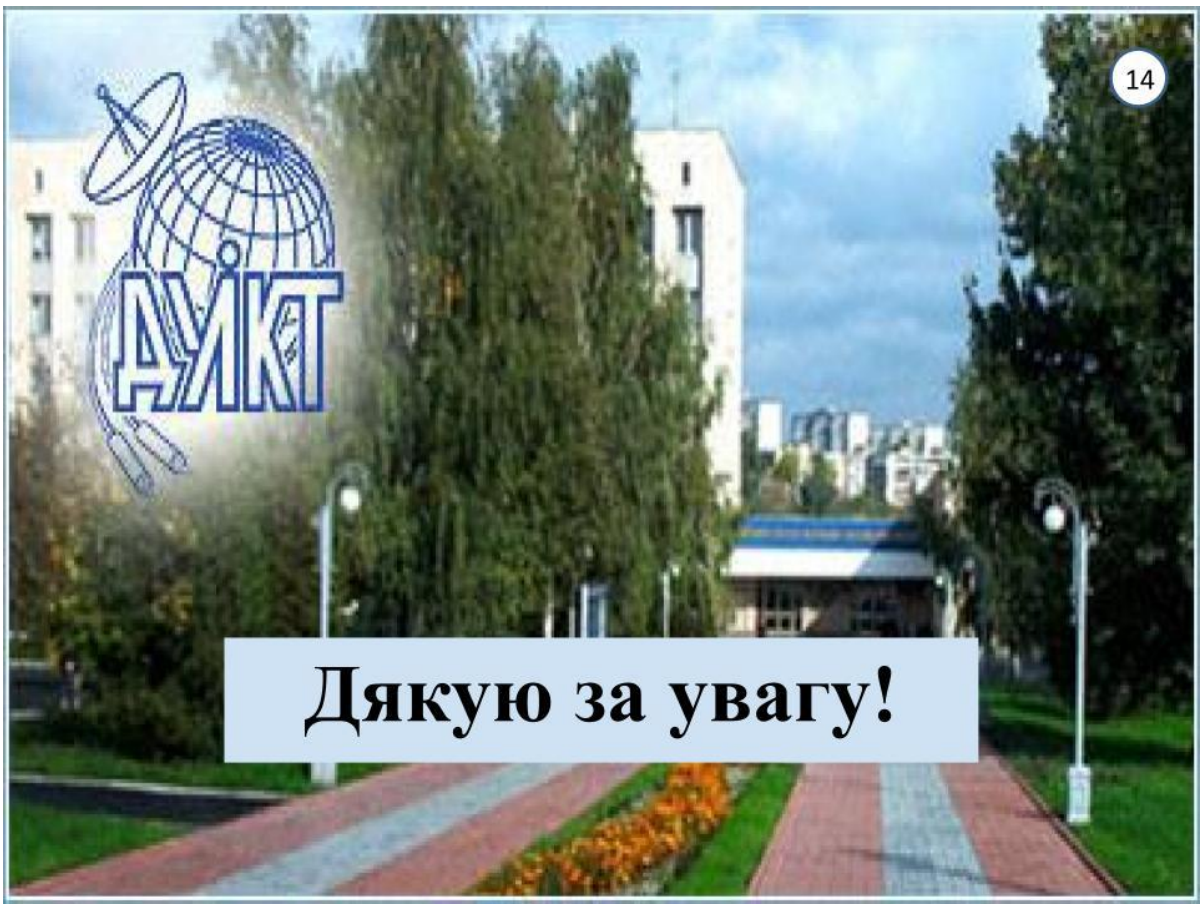
Відстеження підозрілих входів в обліковий запис. Можна відзначати нехарактерні пов'язані з аутентифікацією події, які можуть означати несанкціонований доступ до аккаунту (в тому числі дивні входи в систему і веб-сеанси, вироблені з незвичайних географічних точок).

Відстеження дій на різних платформах. Можна аналізувати дані про поведінку користувачів в різних хмарних додатках (в тому числі SaaS, IaaS, PaaS і IDaaS), щоб отримати взаємопов'язані і всебічні висновки про безпеку.

ВИСНОВКИ

13

- В роботі проведено дослідження та аналіз проблеми забезпечення захисту хмарного середовища як складової частини корпоративної інформаційної системи, встановлена сутність завдань їх захисту.
- Проаналізовано існуючі технології захисту хмарного середовища. Досліджена технологія управління кібербезпекою хмарного середовища на прикладі рішень Cisco Cloudlock.
- Визначено методи та засоби забезпечення управління кібербезпекою хмарного середовища на базі рішень Cisco Cloudlock.
- Встановлено основні функції та принципи роботи програмного комплексу Cisco Cloudlock – це програмне забезпечення, яке призначене для захисту хмарного середовища від новітніх загроз. Для виконання цих завдань програмне забезпечення Cisco Cloudlock має встановлюватися на кожній окремій хмарі. У хмарному середовищі, тобто інформаційній системі налаштовуються функції та політики, здійснюється керування ними за допомогою комплексу Cisco Cloudlock.
- Розроблено рекомендації фахівцям кібернетичної безпеки щодо застосування технології захисту хмарного середовищі у корпоративному сегменті.
- Таким чином, правильна реалізація технології захисту хмарного середовища на базі рішень Cisco Cloudlock має забезпечити ефективний захист та кібербезпеку хмарного середовища.


14
ДУІКТ
Дякую за увагу!