COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.108

УДК 004.75; 004.8

КОНЦЕПЦІЯ АВТОМАТИЗОВАНОЇ ПЕРЕВІРКИ ВІДПОВІДНОСТІ ЯК ОСНОВА ФУНДАМЕНТАЛЬНОЇ МОДЕЛІ ХМАРНОЇ БЕЗПЕКИ

Є. В. Марценюк, А. І. Партика

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: yevhenii.v.martseniuk@lpnu.ua, andrii.i.partyka@lpnu.ua

Основною метою цього дослідження є розробка вдосконаленого автоматизованого методу налаштування та керування публічними обліковими записами та підписками на відомих платформах, таких як AWS, GCP і Azure. Цей метод передбачає застосування стандартизованих конфігурацій для забезпечення оптимальної продуктивності та відповідності вимогам безпеки. Важливим компонентом цієї методології є періодичне сканування інфраструктури хмарних облікових записів і підписок. Це сканування ретельно розроблено для виявлення та розв'язання будь-яких відхилень або проблем невідповідності загальновизнаним стандартам безпеки, включно з NIST 800-53, ISO 27001, HIPAA та PCIDSS.

Цей підхід використовує передові технології автоматизації для оптимізації розгортання та керування хмарними ресурсами. Завдяки автоматизації застосування конфігурацій метод спрямований на зменшення ручних зусиль, мінімізацію ймовірності людської помилки та підвищення ефективності роботи. Ця автоматизація поширюється на процеси безперервного моніторингу та авдиту, даючи змогу в реальному часі виявляти дрейфи конфігурації або вразливості безпеки. Крім того, дослідження спрямоване на розробку динамічної системи, що швидко реагує, здатної адаптуватися до мінливих вимог хмарної безпеки. Компонент автоматизованого сканування відіграє основну роль у цьому аспекті, забезпечуючи постійну впевненість у дотриманні хмарних середовищ найсуворіших протоколів і стандартів безпеки.

Постійний моніторинг відповідності має вирішальне значення в сучасному цифровому середовищі, яке постійно змінюється, де загрози безпеці та конфіденційності даних стають дедалі складнішими. Завдяки інтеграції цих автоматизованих процесів запропонований метод обіцяє не тільки підвищити рівень безпеки хмарних середовищ, але й запропонувати масштабоване та ефективне рішення для керування хмарною інфраструктурою. Цей автоматизований підхід має на меті встановити новий стандарт у хмарному управлінні, узгоджуючи його з найкращими практиками IT-безпеки та відповідності, і відкриваючи шлях для більш безпечних, керованих і ефективних практик хмарних обчислень.

Ключові слова: хостинг, стандарти кібербезпеки, автоматизація, хмарні технології, безпека в публічних хмарних хостингах, оптимізація витрат.

Вступ

На сьогодні більша частина хмарних середовищ потребує впровадження механізмів обліку, контролю зовнішнього периметра безпеки, контролю витрат і моніторингу спеціалістами з кібербезпеки. Здебільшого підхід до процесу перевірки конфігурацій для створення хмарного середовища однаковий і типовий за послідовністю дій. Виходячи з цього, цей процес можна автоматизувати, щоб заощадити час і гроші на створенні того, що вже було створено не раз.

З розвитком технологій хмарних обчислень сфера інформаційних технологій переживає значні трансформації, що потребують нових підходів та рішень для гарантування безпеки та ефективності. Хмарні платформи, такі як Amazon Web Services, Google Cloud Platform та Microsoft Azure, постійно розширюють свої можливості, вводячи нові інструменти та служби для кращого управління ресурсами і безпекою. Ці рішення охоплюють різноманітні функції для масштабування, моніторингу та автоматизації, які спрощують управління інфраструктурою і підвищують її відмовостійкість.

Крім того, зростання кількості кіберзагроз створює потребу для більш глибокого та системного підходу до безпеки, зокрема через застосування політик безпеки, шифрування даних та комплексного авдиту. У відповідь на ці виклики організації інвестують у розробку рішень, які дають змогу автоматично виявляти та реагувати на загрози, забезпечуючи цілісність і конфіденційність корпоративних даних. У цьому контексті, ефективне використання хмарних ресурсів та управління ними є основним для досягнення більшої ефективності та виживання на ринку.

Огляд літературних джерел

У контексті залежності від хмарних технологій, які зростають, питання кібербезпеки стає все більш актуальним. Серед обраних джерел особливо виділяються п’ять з них, які глибоко занурюються в аспекти безпеки, автоматизації та управління хмарними ресурсами.

Дослідження [1] надає комплексний аналіз методів управління безпекою та відповідністю в хмарних середовищах. Автори обговорюють різні підходи до гарантування безпеки, включно з автоматизацією процесів аудиту та відповідністю, що робить це джерело особливо корисним для розуміння інтегрованих стратегій управління.

Автори дослідження [2] зосереджуються на інтеграції систем підтримки ухвалення рішень для кращого захисту інформації. Воно важливе для розуміння, як автоматизація та інтелектуальні системи можуть сприяти покращенню кібербезпеки.

В праці [3] детально проаналізовано проблеми безпеки, які виникають у хмарних обчисленнях, надаючи цінний огляд потенційних ризиків та методів їх управління.

Проблематика статті [4] присвячена застосуванню систематичного підходу PRISMA для огляду алгоритмів безпеки у хмарних середовищах, що допомагає краще зрозуміти ландшафт досліджень у цій галузі та визначити основні напрямки для подальших розробок.

Дослідження [5] зосереджене на використанні систем управління інформацією про безпеку та події (SIEM) для виявлення загроз від інсайдерів. Це важливий компонент у цілісній стратегії кібербезпеки.

Оглянута проблематика робіт формує глибокий аналіз сучасних викликів та рішень у сфері кібербезпеки хмарних технологій. Вони не тільки розкривають різні аспекти технічної та стратегічної безпеки, але й підкреслюють значення автоматизації та інтегрованих підходів.

Мета цієї роботи – створення сервісу для автоматичного застосування конфігурацій для створення хмарного середовища, його обліку у системі внутрішнього обліку організації, обліку доступу користувачів, контролю засобами моніторингу через логи фінансового моніторингу, витрачених сервісами хмарного середовища, конфігурації зовнішнього периметра безпеки та налаштування процесу контролю за критичними вразливими місцями та невідповідністю стандартам безпеки спеціалістами з кібербезпеки [1].

Хмарна безпека є критично важливим аспектом сучасної інфраструктури інформаційних технологій, особливо в контексті все більшої залежності від хмарних обчислень як для бізнесу, так і для персональних додатків [2]. Технології хмарних обчислень мають власні рішення безпеки, але ці рішення надаються лише провайдером, і це є недоліком наявної системи безпеки хмарних обчислень. Клієнт або організація не мають жодних відомостей про те, де зберігаються їхні дані, а

також не мають доступу та контролю над статусом даних. Кожну транзакцію контролює сторона сервера (або провайдера) [3].

Створення IT-сервісів на основі публічної хмарної інфраструктури підкреслює потребу точного контролю та видимості в дуже динамічних середовищах. Хмарними службами, які стають частиною бізнес-додатків і процесу розробки, не можна керувати застарілими IT-технологіями, обмежуючи їх використання лише попередньо визначеними конфігураціями, мережевими топологіями та статично розподіленими ресурсами.

Ця робота присвячена і пропонує спиратися на сучасні інструменти, спеціально створені для обробки конфігурації хмарної платформи та потоків подій, а також динамічного відстеження відповідності безпеки, уразливості конфігурації хмари та стану використання ресурсів. Широке використання організованої автоматизації через API платформи забезпечує послідовне уявлення про хмарні ресурси та пов'язані служби на будь-якому етапі життєвого циклу середовища.

1. Постановка завдання

Сканування конфігурації відіграє життєво важливу роль в управлінні хмарним середовищем, забезпечуючи дотримання критично важливих стандартів кібербезпеки, виявляючи вразливості та ризики на ранніх стадіях для швидкого виправлення, підтримуючи загальну цілісність і надійність системи, забезпечуючи безперервний моніторинг у динамічних хмарних налаштуваннях, сприяючи ретельним процесам аудиту та відповідності, підвищуючи операційну ефективність за допомогою автоматизації, зменшуючи пов'язані з цим ручні перевірки та потенційні витрати на простої, а також значне зміцнення довіри клієнтів та зацікавлених сторін завдяки очевидній прихильності до безпеки та конфіденційності даних. Крім того, у захисті від кіберзагроз, що розвиваються. В умовах постійно мінливого ландшафту ризиків кібербезпеки проактивне сканування дає змогу організаціям випереджати потенційні загрози, виявляючи та усуваючи прогалини в безпеці до того, як вони будуть використані. Ця проактивна позиція має вирішальне значення в той час, коли кібератаки стають все більш витонченими та частими.

Окрім переваг безпеки, сканування конфігурації значно допомагає оптимізувати ресурси та керувати витратами. Постійний аналіз хмарних середовищ допомагає виявити недостатньо використовувані або неефективно налаштовані ресурси, даючи змогу організаціям оптимізувати свої витрати на хмару та розподіл ресурсів. Така фінансова обачність особливо важлива під час масштабного розгортання хмарних об'єктів, де неконтрольоване використання ресурсів може призвести до значних непотрібних витрат.

Ще одним основним аспектом є його роль у забезпеченні відповідності нормативним вимогам. У зв'язку зі щораз вищими нормативними вимогами, особливо в галузях, які обробляють конфіденційні дані, сканування конфігурації гарантує, що хмарні середовища відповідають таким нормам, як GDPR, HIPAA та інші. Ця відповідність є не лише юридичною потребою, а й етичним зобов'язанням захищати дані користувачів, зміцнюючи репутацію організації на ринку. Крім того, сканування конфігурації сприяє більш оптимізованому та гнучкому робочому процесу IT. Автоматизувавши виявлення проблем конфігурації та звітування про них, IT-команди можуть зосередитися на більш стратегічних завданнях, а не загрузнути в рутинних перевірках. Цей перехід до більш стратегічного фокусу є невід'ємною частиною стимулювання інновацій та збереження конкурентоспроможності в цифровому ландшафті.

Врешті сканування конфігурації підвищує готовність до аварійного відновлення. Регулярно перевіряючи та переконуючись, що хмарні середовища налаштовані правильно, організації можуть забезпечити швидший час відновлення у разі аварії. Ця готовність має важливе значення для підтримки безперервності бізнесу та мінімізації впливу будь-яких непередбачених подій. Підсумовуючи, сканування конфігурації є не просто технічною потребою, а стратегічним активом в управлінні хмарним середовищем. Воно відіграє вирішальну роль у кібербезпеці, дотриманні нормативних вимог, управлінні витратами, операційній ефективності та аварійному відновленні, що робить його незамінним інструментом для організацій, які використовують хмарні технології.

2. Аналіз типових загроз безпеки хмарного середовища

Основна проблема безпеки в хмарних середовищах у тому, що відповідальність за безпеку розподіляється між постачальником і користувачем. Більшість провайдерів пропонують доступ до своїх послуг без увімкнених елементів керування безпекою, що добре для процесу розробки послуг, але створює вразливість для безпеки та витік даних із хмарних середовищ [4]. Конфіденційність даних також стає все більш важливою для користувачів і державних установ. Відповідно до Загального регламенту захисту даних (GDPR) і Закону про перенесення та підзвітність медичного страхування (HIPAA), організації мають збирати інформацію прозоро та впроваджувати політики, які допомагають запобігти крадіжці даних або зловживанню. Недотримання цих вимог може призвести до значних збитків і завдати шкоди репутації організації [5].

Організації використовують хмарні обчислення та інструменти хмарної співпраці або обміну повідомленнями для обміну файлами та інформацією з колегами та партнерами. Водночас вони можуть поставити під загрозу регульовані дані та інтелектуальну власність (ІВ), наприклад, комерційну таємницю, інженерні розробки та інші конфіденційні корпоративні дані.

Інфраструктура хмарних обчислень потребує захисту від кіберзагроз. Хмарна безпека – це розділ кібербезпеки, який працює над цим завданням. Хмарна безпека не тільки важлива для захисту даних, але й допомагає галузям і організаціям відповідати вимогам дотримання, захищати від шкоди репутації, забезпечувати безперервність бізнесу в разі руйнівних подій і навіть надавати конкурентну перевагу в умовах високої хмарності [6]. Хмарна безпека має важливе значення, щоб допомогти організаціям усунути конкретні вразливості та загрози. Недбалість або недостатня підготовка співробітників можуть створити загрози безпеці в хмарі, наприклад, передавати файли через загальнодоступні посилання, до яких може отримати доступ кожен. Крадіжка даних інсайдерами також поширена. Наприклад, продавці, які залишають вашу компанію, можуть викрасти дані з хмарних служб CRM [7].

Тіньові IT – це використання хмарних додатків і служб без явного дозволу IT. Користувачі зазвичай використовують несхвалені програми на кшталт “програмне забезпечення як послуга” (SaaS) для обміну файлами, соціальних мереж, співпраці та вебконференцій. Користувачі, які завантажують корпоративні дані в несхвалені програми, можуть порушити правила конфіденційності даних і проживання.

Є ще одна складна проблема: сторонні програми та сценарії з дозволами OAuth. Підключені до OAuth програми сторонніх розробників отримують доступ до схвалених IT-сервісів хмарних обчислень, таких як Microsoft Office 365 і Google G Suite. Зазвичай у хмарному середовищі організації можна побачити сотню, якщо не тисячу програм і сценаріїв. Деякі створюють ризики через поганий дизайн, надаючи їм ширші, ніж потрібні, дозволи на дані. Деякі з них шкідливі або їх легко використовувати [8]. Чим небезпечний OAuth? Після авторизації маркера OAuth доступ до корпоративних даних і додатків продовжується до скасування [9].

Основною метою цієї статті є розгляд стратегій та інструментів для забезпечення безпеки в хмарних середовищах, а також розроблення концепції автоматизованої перевірки відповідності як основи фундаментальної моделі хмарної безпеки. Конкретні завдання дослідження вміщають:

- Аналіз зобов’язань щодо безпеки та конфіденційності, визначених постачальниками хмарних середовищ.
- Дослідження інструментів, які гарантують безпечний доступ до хмари, щоб контролювати всі програми та дані, які використовує організація (Azure Active Directory, AWS Identity, Google Authenticator, Okta).
- Розгляд інструментів для керування хмарною безпекою, які можуть виявляти та виправляти помилки конфігурації (Prisma Cloud, Vanta).
- Аналіз можливостей впровадження платформи захисту хмарної інфраструктури та її інтеграція в процес розробки, з врахуванням регулярного оновлення та впровадження політик безпеки (захист кінцевої точки).

- Оцінка ефективності процесу навчання співробітників щодо принципів безпеки організації та можливостей фішингу.
- Розгляд стратегії захисту на основі моделі “нульової довіри” і використання системи керування ідентифікацією та доступом для критичних вузлів інфраструктури.

Фундаментальність моделі полягає в тому, що дає змогу систематично дослідити та розглянути основні аспекти безпеки та контролю інфраструктури хмарних середовищ і забезпечити безперервний автоматизований цикл покращення конфігурацій згідно із світовими стандартами безпеки (NIST 800-53, HIPAA, PCI-DSS, SOC, ISO), що має велике значення як для академічної спільноти, так і для практичного застосування в сучасному бізнес-середовищі.

2. Концепція “безперервного автоматизованого сканування конфігурацій” як основний елемент захисту хмарних середовищ

Незважаючи на наявність численних інструментів, більшій частині організацій складно ефективно контролювати доступ до своїх даних і впроваджувати політики безпеки в хмарних середовищах, що постійно змінюються. Крім того, забезпечення відповідності під час зберігання даних в розподілених середовищах створює значне навантаження на фахівців і без того обмежені команди безпеки [10].

2.1 . Моделі надання хмарних послуг та їх особливості

IaaS, PaaS, and SaaS – це три найпопулярніші типи пропозицій хмарних послуг. Іноді їх називають моделями хмарних сервісів або моделями послуг хмарних обчислень.

- **IaaS**, або “infrastructure as a service”, інфраструктура як послуга – це доступ на вимогу до розміщених у хмарі фізичних і віртуальних серверів, сховищ і мереж – серверної IT-інфраструктури для запуску додатків і робочих навантажень у хмарі.
- **PaaS**, що розшифровується як “Platform as a Service” (платформа як послуга), надає користувачам доступ до повнофункціональної хмарної платформи на вимогу. Ця платформа дає змогу розробникам створювати, запускати, тестувати, обслуговувати та керувати програмними додатками без витрачання часу та ресурсів на придбання, управління та підтримку фізичної або віртуальної інфраструктури, що потрібна для їхньої роботи.
- **SaaS**, або “software as a service”, програмне забезпечення як послуга – це доступ на вимогу до готового до використання прикладного програмного забезпечення, розміщеного у хмарі.

IaaS, PaaS і SaaS не є взаємовиключними. Багато середніх підприємств використовують більше одного, а більша частина великих підприємств використовує усі три (рис. 1).

“Як послуга” означає спосіб споживання IT-активів у цих пропозиціях, а також істотну різницю між хмарними обчисленнями та традиційними IT. У традиційних IT організація споживає IT-активи – апаратне забезпечення, системне програмне забезпечення, засоби розробки, додатки, купуючи їх, встановлюючи, керуючи ними та підтримуючи у власному локальному центрі обробки даних. У хмарних обчисленнях постачальник хмарних послуг володіє, керує та обслуговує активи; клієнт споживає їх через інтернет-з’єднання та оплачує за підпискою або з оплатою за фактом використання.

Отже, головною перевагою IaaS, PaaS, SaaS або будь-якого іншого рішення “як послуга” є економічна: клієнт може отримати доступ до потрібних йому IT-можливостей та масштабувати їх за передбачувану ціну, без витрат та накладних витрат, пов’язаних із закупівлею та обслуговуванням усього у власному центрі обробки даних. Але є додаткові переваги, характерні для кожного з цих рішень [11].

2.2 . Безперервне автоматизоване сканування конфігурацій

Автоматизований процес використовує центральний оркестратор, який виконує ініціалізацію та зміни в хмарі IaaS та допоміжних сервісах. Він заснований на платформі Rundeck і бібліотеці сценаріїв, що складається з відомого набору інструментів автоматизації IT, Ansible [12] і Python [13]. Самі сценарії підтримуються і розвиваються в процесі розробки КІ з контролем коду і тестуванням.

Оркестратор і структура сценаріїв розроблені таким способом, щоб не зберігати жодних даних про хмарні середовища, які вони контролюють. Усі потрібні дані для виконання завдання та статусу завдання передаються до та з Rundeck через REST API. Це рішення використовується для полегшення масштабування та задоволення вимог до доступності та безпеки системи. Безпека оркестратора під час оцінки хмарних середовищ може бути посилена за допомогою служб зберігання секретної інформації, таких як HashiCorp Vault [14].

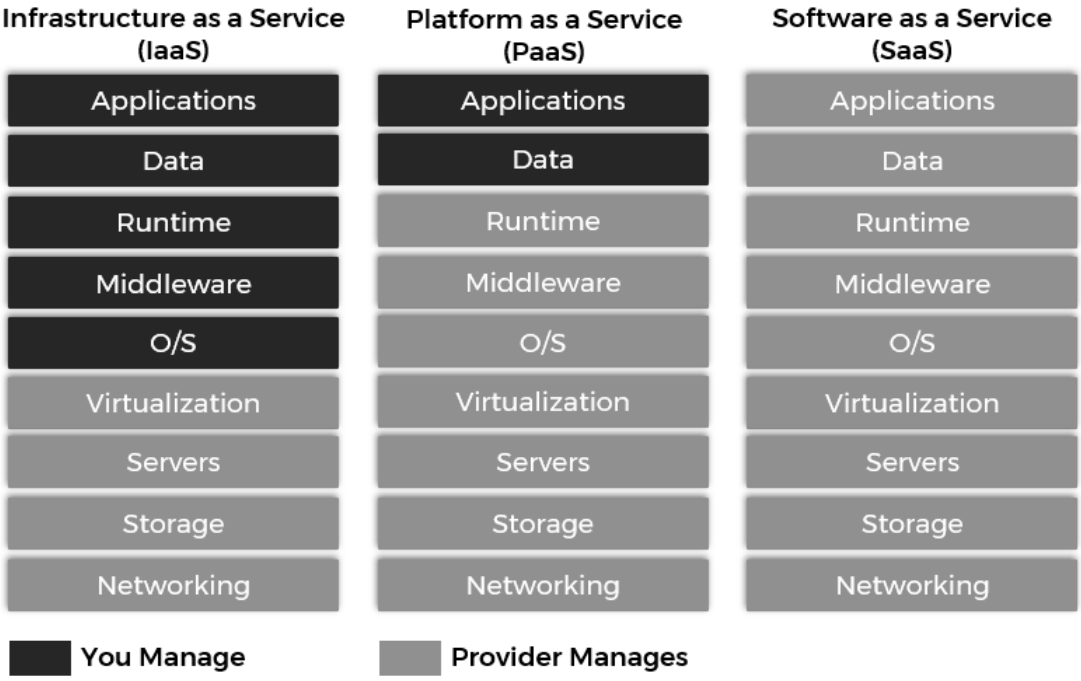

Рис. 1. Управління ресурсами в хмарних обчисленнях

Сканування конфігурації – це процес виявлення невідповідностей у конфігурації на основі журналів хмарного середовища (Audit logs, Flow logs) та порівняння конфігурації з рекомендованими стандартами кібербезпеки (NIST 800-53, HIPAA, PCI-DSS, SOC, ISO) [15].

Використовуючи безперервну інтеграцію за допомогою авдиту та реєстрації потоків між хмарними середовищами та Prisma, система забезпечує безперервний моніторинг та відповідність. Ця інтеграція полегшує видимість хмарної інфраструктури в режимі реального часу, даючи можливість негайно виявляти та виправляти будь-які відхилення від встановлених стандартів безпеки або операційних контрольних показників. Підхід до безперервної інтеграції не тільки підвищує безпеку, але й забезпечує операційну ефективність і надійність.

Крім того, система використовує розширену аналітику для інтерпретації даних журналів, надаючи уявлення про моделі використання та потенційні вразливості. Такий підхід, заснований на даних, дає змогу проактивно виявляти ризики безпеки та операційну неефективність. Застосовуючи алгоритми машинного навчання, система може прогнозувати потенційні проблеми на основі історичних даних, полегшуючи превентивні дії для зниження ризиків.

На додаток до безпеки та операційної ефективності дизайн системи надає пріоритет гнучкості та адаптивності. Це досягається за допомогою модульної архітектури сценаріїв, що дає змогу швидко коригувати і налаштовувати відповідно до мінливих потреб бізнесу та технологічного прогресу. Використання Ansible і Python гарантує, що система залишається в авангарді технологій автоматизації, користуючись широкою підтримкою та постійними оновленнями, які ці інструменти отримують від відповідних спільнот.

Завдяки безперервній інтеграції за допомогою авдиту та реєстрації потоків між хмарними середовищами і Prisma Cloud було досягнуто безперервного контролю над конфігураціями, зовнішнім периметром, витратами, управлінням змінами, авторизацією та погодженням цих активів із відповідними стандартами безпеки (рис. 2).

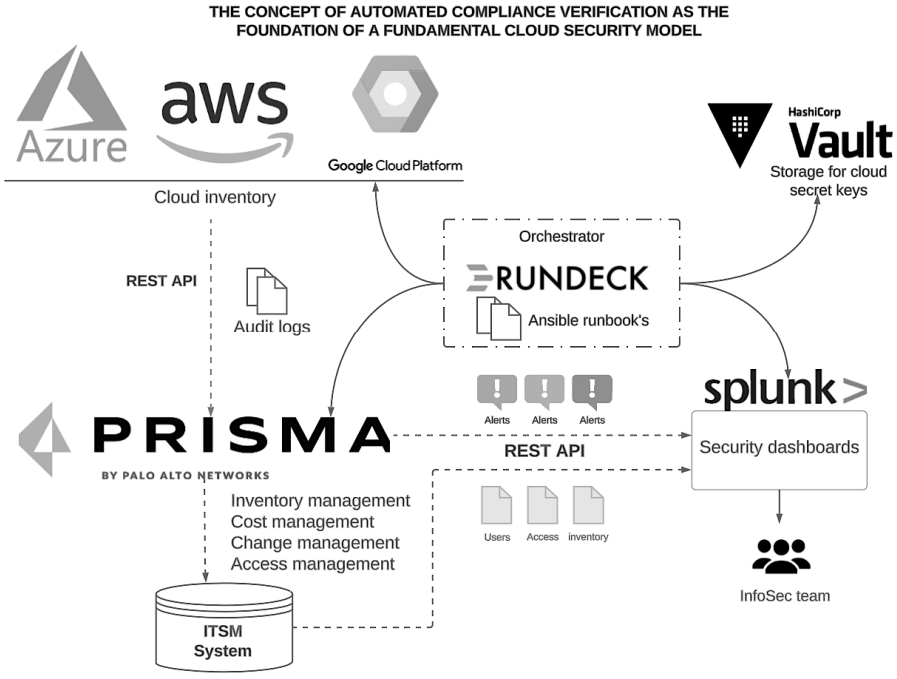

Рис. 2. Автоматизоване сканування технологічної схеми конфігурацій

2.3 . Основні переваги автоматизованого підходу

Виявлення невідповідностей: сканування конфігурації ефективно виявляє розбіжності та невідповідності в налаштуваннях хмари, аналізуючи журнали середовища. Це проактивне виявлення має вирішальне значення для підтримки цілісності та безпеки хмарних інфраструктур.

Відповідність стандартам безпеки: порівнюючи поточні конфігурації з усталеними стандартами кібербезпеки, такими як NIST 800-53, HIPAA, PCIDSS, SOC та ISO, сканування конфігурації забезпечує дотримання цих критично важливих вказівок, підвищуючи загальну відповідність вимогам безпеки.

Безперервна інтеграція та моніторинг: інтеграція сканування конфігурації в процесі безперервної інтеграції (CI) за допомогою таких інструментів, як Ansible, Python і Prisma Cloud, дає змогу здійснювати постійний моніторинг і контроль над конфігураціями хмари. Цей безперервний підхід є ключем до підтримки безпечних та ефективних хмарних середовищ.

Покращений стан безпеки: завдяки використанню передових інструментів і методів, зокрема аудиту і реєстрації потоків, процес сканування сприяє зміцненню безпеки, керуючи зовнішнім периметром, відстежуючи витрати і контролюючи процеси управління змінами та авторизації.

Підвищена безпека даних: використання таких сервісів, як HashiCorp Vault, для зберігання конфіденційної інформації, а також дизайн оркестраторів таким способом, щоб вони не зберігали дані хмарного середовища безпосередньо, посилює безпеку процесу сканування конфігурації, гарантуючи, що конфіденційні дані залишаються захищеними.

Масштабованість і надійність: система сканування конфігурації розроблена для масштабованості та високої доступності. Використання REST API з Rundeck для зв'язку гарантує, що система може ефективно масштабуватися, відповідаючи суворим вимогам безпеки та доступності.

2.4 . Аналіз витрат та фінансові вигоди від використання автоматизованого сканування конфігурації

Зниження експлуатаційних витрат: однією з найважливіших переваг автоматизованого сканування конфігурації є зниження експлуатаційних витрат. Автоматизуючи планові перевірки та технічне обслуговування, організації можуть значно скоротити час і трудовитрати, пов'язані з ручним переглядом конфігурації. Ця автоматизація призводить до прямої економії коштів, оскільки для виконання цих завдань потрібно менше часу персоналу, що дає змогу персоналу зосередитися на більш стратегічних ініціативах.

Запобігання додатковим витратам: автоматизоване сканування конфігурації відіграє вирішальну роль у виявленні потенційних вразливостей до того, як вони можуть бути використані зловмисниками. Ціна витоку даних або інциденту безпеки може бути значною не лише з погляду фінансових втрат, але й репутаційної шкоди. Раннє виявлення та усунення вразливостей за допомогою автоматизованого сканування може запобігти цим дорогим інцидентам, забезпечуючи значну віддачу від інвестицій.

Оптимізація використання ресурсів: автоматичне сканування допомагає виявити надмірно розподілені або недостатньо використані ресурси в хмарному середовищі. Оптимізуючи ці ресурси, організації можуть досягти значної економії коштів на своїх витратах на хмару. Ефективне використання ресурсів не тільки знижує витрати, але й підвищує загальну продуктивність хмарних сервісів.

Зниження витрат на відповідність: недотримання нормативних стандартів може призвести до великих штрафів і юридичних наслідків. Автоматизоване сканування конфігурації забезпечує постійну відповідність різним галузевим стандартам, таким способом уникаючи витрат, пов'язаних із недотриманням. Ця постійна відповідність вимогам є не тільки заходом економії коштів, але й зміцнює позиції організації в регульованих галузях.

Збільшення часу безвідмовної роботи системи: підтримуючи оптимальні налаштування конфігурації, автоматичне сканування сприяє збільшенню часу безвідмовної роботи та надійності системи. Простої можуть бути неймовірно дорогими для бізнесу, як з погляду втраченого доходу, так і витрат на відновлення. Стабільність, що забезпечується послідовним скануванням конфігурації, мінімізує ризик простоїв, таким способом захищаючи від цих потенційних втрат.

Довгострокові стратегічні переваги: впровадження автоматизованого сканування конфігурації узгоджується з довгостроковими стратегічними перевагами. Це сприяє формуванню культури ефективності, безпеки та дотримання вимог в організації. Ці переваги хоч і не піддаються прямій кількісній оцінці в короткостроковій перспективі, сприяють загальному здоров'ю та конкурентоспроможності бізнесу в довгостроковій перспективі [16].

Аналіз витрат та переваг автоматизованого сканування конфігурації показує переконливі аргументи на користь його впровадження. Початкові інвестиції в такі системи переважуються значною економією операційних витрат, запобіганням дорогим порушенням, оптимізацією ресурсів, зниженням витрат на дотримання нормативних вимог, збільшенням часу безвідмовної роботи системи та довгостроковими стратегічними перевагами. Цей аналіз підкреслює важливість автоматизованого сканування конфігурації як життєво важливого компонента в сучасних стратегіях управління хмарою.

3. Огляд компонентів, які використано для практичної реалізації концепції

Prisma Cloud™ – це продукт PaloAlto Networks, який дає змогу відстежувати конфігурації, порівнювати їх зі стандартами безпеки, аналізувати конфігурацію хмарних сервісів, виявляти ризики, виконувати автоматичні корекції конфігурації відповідно до встановлених політик безпеки.

Автоматизоване сканування використовує спеціалізовану службу Prisma Public Cloud для безперервної перевірки конфігурації хмарних середовищ, відстеження історії активів і контролю дій адміністратора. Процес управління відповідністю, реалізований в Prisma Public Cloud, порівнює

конфігурацію платформи з вимогами стандартів інформаційної безпеки і попереджає SIEM-систему про випадки невідповідності. Він також надає сповіщення про небезпечні дії адміністраторів і необов'язкові звіти про підозрілі мережеві з'єднання, які можуть свідчити про спроби атаки. Кожен хмарний обліковий запис, обраний для перевірки відповідності, має роль доступу для служби Prisma Public Cloud, також відповідні послуги конфігурації та експорту подій. У цьому фреймворку оркестратор Rundeck враховує цей обліковий запис у Prisma Public Cloud і правильно визначає його для відповідного профілю перевірки.

Для перевірки коду та процесів функціональність Prisma Public Cloud також може бути інтегрована з хмарними середовищами на рівні хоста та контейнера. Ця можливість особливо корисна в середовищах, які потребують контролю для безпечної розробки коду продукту. Крім того, Prisma Cloud пропонує покращену видимість і контроль над мультихмарними середовищами. Його всеосяжна інформаційна панель забезпечує уніфіковане уявлення про безпеку та відповідність вимогам на різних хмарних платформах. Цей цілісний підхід має вирішальне значення для організацій, що працюють у гібридних або мультихмарних інфраструктурах, де видимість часто може бути фрагментована. Prisma Cloud має розширені можливості виявлення загроз. Використовуючи штучний інтелект та алгоритми машинного навчання, він може виявляти аномальну поведінку та потенційні загрози в режимі реального часу. Такий рівень розвідки безпеки має вирішальне значення для превентивного виявлення та пом'якшення складних кіберзагроз.

Ще одним важливим аспектом Prisma Cloud є його здатність автоматизувати дії з виправлення. У разі виявлення загрози безпеці або проблеми з відповідністю система може автоматично впровадити попередньо визначені кроки виправлення або надати рекомендації щодо ручного втручання. Ця автоматизація не тільки прискорює час відгуку, але й зменшує ймовірність людської помилки [17].

Prisma Cloud також підтримує створення спеціальних політик, що дає змогу організаціям адаптувати перевірки безпеки та відповідності до своїх конкретних потреб. Це налаштування гарантує, що заходи безпеки не просто широкі та загальні, але й спеціально узгоджені з унікальними вимогами організації та профілем ризику.

Splunk – є лідером на ринку SIEM (Security Information and Event Management), що поєднує дві основні області програмного забезпечення для безпеки: SIM (Security Information Management) – управління інформацією про безпеку та SEM (Security Event Management) – управління подіями безпеки. Це означає, що Splunk надає інструменти для збору, аналізу та інтерпретації даних, пов'язаних з безпекою, даючи змогу організаціям ефективно ідентифікувати, реагувати на інциденти безпеки та моніторити свої IT-інфраструктури для попередження потенційних загроз.

Кожне середовище IaaS, зареєстроване в автоматизованій системі сканування, зазвичай налаштоване на експорт подій платформи в розміщений Splunk SIEM. Операція реєстрації налаштовує відповідні ролі доступу та служби сповіщення про події на стороні платформи IaaS разом із спеціальним індексом Splunk для зберігання та візуалізації даних подій та інформаційних панелей. Користувачам, які мають відповідні ролі доступу в певному хмарному середовищі, може бути автоматично надано доступ до інформаційних панелей Splunk для відповідного середовища.

Існує інтеграція на рівні даних між SIEM і платформою ITSM для експорту в Splunk об'єктів Configuration Item (CI), які описують хмарні середовища і всі пов'язані з ними інциденти. Ця інтеграція спрямована на збагачення подій, які надходять із хмарних платформ, метаданими бізнес-рівня та процесів. Ця можливість використовується для реалізації інформаційних панелей, які відображають інциденти, пов'язані з середовищами, швидкістю їх обробки, класифікацією пріоритетів, впливом на сервіс тощо [18].

Rundeck Rundeck – це платформа автоматизації runbook, яка значно скорочує та оптимізує операційні робочі процеси. Його характеризує простий у використанні інтерфейс користувача, який дає змогу технічному або нетехнічному персоналу адмініструвати та виконувати складні завдання

без спеціальної підготовки. Насправді ця функція є особливо ефективною в критичних за часом середовищах, в яких скорочення часу реагування та самозабезпечення є обов'язковими.

Основною характеристикою цієї платформи є її здатність впроваджувати автоматизацію в складні робочі процеси. Призначена для послідовного виконання операційних завдань і без помилок, відіграє вирішальну роль у підтримці операційної цілісності та ефективності. Стандартизація, запроваджена цим рішенням, має вирішальне значення у великих організаціях, де кілька команд, які працюють над кількома процесами, часто можуть досить легко порушити зв'язок і призвести до розбіжностей. Автоматизація цих рутинних складних завдань вивільняє дорогоцінний час для IT-персоналу, щоб зосередитися на більш стратегічних ініціативах. Це кардинальна зміна, яка робиться для підвищення загальної продуктивності та ефективності команди, переходячи від ручної, повторюваної роботи до діяльності з більшою доданою вартістю.

Rundeck також добре працює, забезпечуючи більший контроль та управління IT-операціями. Він має жорстку детальну функцію реєстрації, яка забезпечує прозорість і підзвітність під час видачі операційних процесів для відстеження в межах управління. До того ж інтеграція з декількома наявними інструментами і системами дає змогу створювати єдині операційні центри, які будуть покращувати роботу з невеликими змінами. У разі безпеки та відповідності всі операційні завдання виконуються за встановленими протоколами та стандартами. Контроль доступу, а також функції контрольного журналу на платформі відіграють вирішальну роль у підтримці безпечного робочого середовища, де немає лазівок для будь-яких потенційних порушень, а також у виконанні нормативних вимог, що висуваються до таких систем [19].

Автоматизація Runbook – це використання програмного забезпечення для автоматизації рутинних, повторюваних і часто складних операційних завдань та процедур в IT-середовищі (рис. 3). Традиційно runbook – це компіляція рутинних процедур і операцій, які виконує системний адміністратор або оператор. Автоматизація цих ранбуків означає використання програмного забезпечення для виконання цих процедур автоматично або з мінімальним втручанням людини.

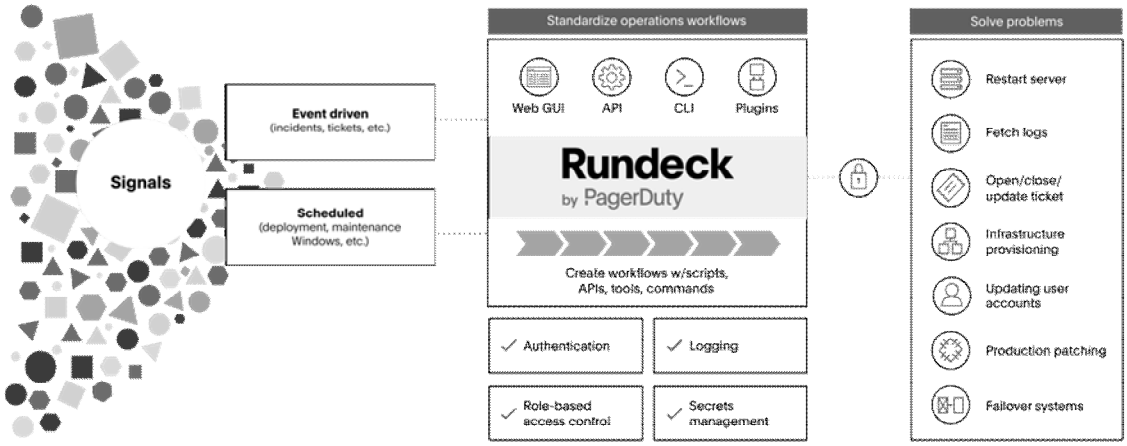

Рис. 3. Процес автоматизації Runbook [20]

Rundeck, як інструмент автоматизації runbook, покращує цей процес, надаючи комплексну та зручну платформу для автоматизації широкого спектру IT-завдань. Це дає змогу IT-командам кодифікувати свої операційні процедури в автоматизовані робочі процеси. Ці робочі процеси можуть варіюватися від простих рутинних завдань до складних, багатоетапних процесів. Отже, Rundeck не тільки скорочує час і зусилля, пов'язані з виконанням цих завдань, але й мінімізує ймовірність людської помилки.

Однією з головних особливостей Rundeck є його здатність інтегруватися з широким спектром інструментів і систем, що робить його універсальним варіантом для багатьох IT-середовищ. Ця можливість інтеграції означає, що Rundeck може керувати складними процесами в різних системах, забезпечуючи злагоджений операційний досвід [20].

HashiCorp Vault розроблений, щоб допомогти організаціям керувати доступом до секретів і безпечно передавати їх у межах організації. Секретні дані визначаються як будь-яка форма конфіденційних облікових даних, які потрібно суворо контролювати та відстежувати і які можна використовувати для розблокування конфіденційної інформації. Секрети можуть бути у вигляді паролів, ключів API, ключів SSH, токенів RSA або одноразових паролів. HashiCorp Vault дає змогу дуже легко контролювати та керувати доступом, надаючи вам односторонній інтерфейс для керування кожним секретом у вашій інфраструктурі. Мало того, ви також можете створювати детальні журнали авдиту та відстежувати, хто до чого звертався [21].

HashiCorp Vault є інструментом для управління секретами, створеним для забезпечення контролю доступу до чутливої інформації в середовищах із низьким рівнем довіри. Він дає змогу зберігати чутливі дані, а також динамічно створювати доступність для окремих сервісів або додатків на основі оренди. Vault також застосовується для аутентифікації користувачів, як машин, так і людей, переконуючись в їх правомірності доступу до визначених ресурсів. Ця аутентифікація може відбуватися через паролі або через використання динамічних значень для створення тимчасових токенів, що надають доступ до специфічних директорій. Для регулювання правил доступу використовуються політики, написані мовою конфігурації HashiCorp (HCL), які точно визначають, хто має доступ до яких ресурсів [22–24].

Управління секретами: HashiCorp Vault виступає як універсальне рішення для управління секретами, пропонуючи безпечне зберігання різноманітних типів конфіденційної інформації, включаючи змінні середовища, облікові дані до баз даних, API ключі та інше. Це дає змогу користувачам мати детальний контроль над тим, кому дозволено доступ до цих секретів. Використання Vault дає можливість не лише зберігати ці дані в безпеці, але й динамічно управляти доступом до них, зокрема обертання ключів та відкликання доступу, коли це потрібно, забезпечуючи високий рівень захисту та контролю над конфіденційними даними.

Замість того, щоб зберігати відкриті текстові файли, щоб їх побачив увесь світ, ви можете зчитувати сховище запитів програми або API HashiCorp, який захищає версії цих файлів у відкритому тексті. Секрети також легко обертати та відкликати. Якщо співробітник залишає вашу організацію, ви можете легко та безпечно відкликати його доступ.

Доступ на основі ідентифікаційних даних: HashiCorp Vault використовує доступ на основі ідентифікаційних даних для брокерського доступу до систем і секретів. Коли справа доходить до аутентифікації за допомогою ідентифікації, є дві основні дійові особи: люди та машини. Управління доступом для людей здійснюється за допомогою контролю доступу на основі ролей (RBAC), надання дозволу та обмеження доступу для створення та керування секретними даними або керування доступом інших користувачів на основі секретного значення, з яким вони ввійшли в систему.

З другого боку, керування доступом для машин передбачає надання доступу до різних серверів або секретів. Завдяки динамічному характеру HashiCorp Vault ви можете створювати секрети, які працюють тимчасово та відкликають доступ у разі злому. Ви можете генерувати секретні дані на вимогу для певної системи, як-от Sensu, AWS або Consul, і генерувати пару ключів із дійсним дозволом. Після використання згенеровані динамічні секрети будуть автоматично відкликані.

Шифрування даних: Vault пропонує послугу “шифрування як послугу”, забезпечуючи шифрування даних як у процесі їх передання, так і в стані спокою. Для шифрування даних, що передаються, використовується TLS, а для даних у стані спокою – 256-бітне шифрування CBC AES. Цей підхід ефективно захищає конфіденційну інформацію від несанкціонованого доступу, як у

момент передання її через мережу, так і під час зберігання в хмарних сховищах чи дата-центрах. Централізоване управління ключами спрощує процес оновлення та розгортання ключів по всій розподіленій інфраструктурі, забезпечуючи зручне та ефективне управління шифруванням [25].

ITSM – система обліку активів організації. Містить інформацію про активи, проєкти, розподіл вартості, зафіксовані зміни, облік системи авторизації та надані доступи [26].

Для автоматизації та оркестрування будь-якого сервісу потрібне надійне джерело записів та сховища метаданих:

– Послуги, які вони містять.

– Ідентифікація та найменування компонентів.

– Відношення до організаційної структури.

– Поточний стан життєвого циклу.

– Елементи конфігурації та залежності, які налаштовуються.

Платформа ITSM зберігає складні структури даних – елементи конфігурації (CI) – для кожного хмарного облікового запису та пов'язаних з ним елементів сервісу. У процесі управління життєвим циклом середовища, у міру модифікації записів CI (реєстрація нового облікового запису, зміна власника облікового запису або налаштування профілю моніторингу), зміни передаються платформі оркестрації через транзакції API, а відповідні модифікації конфігурації вносяться в хмарні служби.

Використання системи ITSM/CMDB (CMDB – Configuration Management Database – база даних конфігурацій) для централізованого зберігання метаданих хмарного середовища гарантує, що всі ресурси надаються послідовно, за потрібною схемою, та завжди мають фактичні зв'язки з пов'язаними сутностями. Крім того, цей централізований підхід до управління метаданими хмарного середовища за допомогою системи ITSM/CMDB відіграє важливу роль у покращенні загального управління та контролю над IT-ресурсами. Це дає змогу структуровано та організовано відстежувати активи впродовж усього їх життєвого циклу, від закупівлі до виведення з експлуатації. Це систематичне відстеження має вирішальне значення для ефективного управління активами, гарантуючи, що кожен актив обліковується та використовується ефективно.

Крім того, інтеграція систем ITSM з хмарними сервісами сприяє кращому управлінню ризиками. Підтримуючи актуальну інвентаризацію активів та їх конфігурацій, організації можуть швидко виявляти потенційні вразливості безпеки або проблеми з відповідністю та реагувати на них. Такий проактивний підхід до управління ризиками має важливе значення для мінімізації впливу загроз безпеці та забезпечення відповідності різним нормативним вимогам. Ще однією основною перевагою використання системи ITSM у поєднанні з хмарними сервісами є покращення процесів управління інцидентами та змінами. Завдяки всебічному огляду всіх активів та їх конфігурацій IT-команди можуть ефективніше діагностувати та усувати інциденти. Крім того, система гарантує, що будь-які зміни в IT-середовищі належно задокументовані та впроваджені, зменшуючи ймовірність помилок або збоїв у роботі служб [27].

Система ITSM також відіграє важливу роль в управлінні фінансами та оптимізації витрат. Надаючи детальну інформацію про використання активів і витрати, організації можуть ухвалювати більш обґрунтовані рішення щодо своїх інвестицій в IT. Така фінансова прозорість є життєво важливою для оптимізації витрат на IT та узгодження IT-ресурсів із бізнес-цілями. Отже, інтеграція систем ITSM з хмарними середовищами дає численні переваги, зокрема покращене управління та контроль, покращене управління ризиками, ефективніше управління інцидентами та змінами, а також кращий фінансовий нагляд. Ці переваги підкреслюють важливість систем ITSM в управлінні сучасною IT-інфраструктурою, особливо в умовах усе більш складних і динамічних хмарних середовищ.

REST API – це набір визначень та протоколів для створення та інтеграції програмного забезпечення. Іноді його називають договором між постачальником інформації та споживачем інформації, який встановлює контент, який запитується у споживача (дзвінок) та контент, який запитує виробник (відповідь) [28].

REST є набором архітектурних обмежень, але не є протоколом чи стандартом. API можуть впроваджувати REST у різноманітних варіаціях. Коли виконується клієнтський запит через RESTful API, він передає стан ресурсу до запитувача або до кінцевої точки. Представлення цього стану доставляється у формі одного з кількох форматів через HTTP, зокрема JSON (Javascript Object Notation), HTML, XLT, Python, PHP або простий текст. З усіх форматів JSON є найбільш вживаним, оскільки він є мовно нейтральним і зрозумілим як для людей, так і для машин [28].

Важливо не забувати, що в HTTP-методах RESTful API заголовки та параметри відіграють основну роль, адже вони несуть критично важливі дані про ідентифікатори, метадані запиту, авторизацію, URI (уніфікований ідентифікатор ресурсу), кешування, cookies та інше. Існують як заголовки для запитів, так і для відповідей, кожен з яких містить унікальну інформацію, пов'язану з HTTP-сесією та кодами статусу.

Щоб вважатися RESTful, API має задовольняти такі критерії:

1. Архітектура клієнт-сервер: включає клієнтів, сервери та ресурси, з управлінням запитів через HTTP.
2. Безстатусне зв'язкування між клієнтом та сервером, де інформація про клієнта не зберігається між запитами, роблячи кожен запит незалежним.
3. Кешування даних для оптимізації взаємодії між клієнтом і сервером.
4. Єдиний інтерфейс між компонентами для стандартизованого передання інформації, з вимогами:

- Можливість ідентифікації та відділення запитуваних ресурсів від представлень, надісланих клієнту.
- Здатність клієнта маніпулювати ресурсами через отримані представлення, які містять достатньо інформації для цього.
- Повернення самоописних повідомлень з достатньою інформацією для клієнта, щоб розуміти, як обробляти їх.
- Наявність гіпертексту/гіпермедіа, даючи змогу клієнтові використовувати гіперпосилання для виявлення усіх доступних дій, які можна виконати після доступу до ресурсу.

5. Багаторівнева система, що дає можливість організовувати сервери за типами (безпека, балансування навантаження тощо) і передбачає непомітне для клієнта отримання інформації в ієрархічній структурі.

Ще дещо, про що треба пам'ятати: заголовки та параметри також важливі в методах HTTP RESTful API HTTP-запиту, оскільки вони містять важливу інформацію про ідентифікатор щодо метаданих запиту, авторизації, уніфікованого ідентифікатора ресурсу (URI), кешування, файлів cookie тощо. Існують заголовки запитів і заголовки відповідей, кожен з яких має власну інформацію про HTTP-з'єднання та коди стану.

6. Code-on-demand (не обов'язкова опція): можливість відправляти виконуваний код з сервера клієнту за запитом, розширюючи функціональність клієнта.

Результати дослідження

Етап тестування цього дослідницького проєкту був комплексно проведений з використанням інфраструктур основних хмарних середовищ, зокрема Azure, AWS та GCP. Цей різноманітний вибір платформ відіграв важливу роль у підтвердженні універсальності та ефективності автоматизованого методу конфігурації та сканування в різних хмарних екосистемах. Кожне з цих хмарних середовищ має унікальні характеристики та проблеми, що робить їх ідеальними для ретельного та надійного процесу тестування.

В Azure тестування було зосереджено на оцінці того, наскільки добре автоматизований метод інтегрується з його рідними інструментами та службами, особливо з погляду управління конфігурацією та відповідності стандартам безпеки. AWS, з його широкими пропозиціями послуг і складною інфраструктурою, забезпечив широкий випробувальний полігон для оцінки масштабованості

та адаптивності методу. Тестування в GCP було спрямоване на аналіз ефективності автоматизації в середовищі, орієнтованому на Google, особливо з огляду на різні інструменти безпеки та управління GCP.

Під час тестування були змодельовані різні сценарії, щоб охопити широкий спектр можливих конфігурацій, проблем безпеки та вимог відповідності. Це розгортання різних типів хмарних ресурсів, застосування різних налаштувань конфігурації, а пізніше проведення періодичного сканування для виявлення будь-яких невідповідностей зазначеним світовим стандартам безпеки, таким як NIST 800-53, ISO 27001, HIPAA та PCIDSS.

Тестування також містило моніторинг реакції автоматизованої системи на індуковані зміни конфігурації та потенційні порушення безпеки. Це дало цінну інформацію про здатність системи оперативно виявляти та усувати невідповідні конфігурації та вразливості, таким способом забезпечуючи постійне дотримання найвищих стандартів безпеки.

Висновки

У цій роботі запропоновано і розроблено сервіс, який може бути використаний як механізм для безперервного та автоматизованого контролю облікових записів/підписок у хмарних середовищах, таких як Azure (Microsoft), AWS (Amazon) та GCP (Google). Сервіс складається з таких модулів:

- Модуль керування конфігурацією: цей модуль відповідає за те, щоб хмарні середовища відповідали заздалегідь визначеним стандартам безпеки. Він проводить базові перевірки на відповідність і підтримує потрібні стандарти конфігурації.
- Модуль обліку та аудиту: містить компоненти для керування доступом користувачів, встановлення лімітів витрат, відстеження змін та моніторингу терміну служби активів. Цей модуль є основним для ведення точного обліку та забезпечення відповідності фінансовим вимогам і вимогам, пов’язаним із доступом.
- Модуль звітності та сповіщень: цей модуль призначений для полегшення спілкування з фахівцями з кібербезпеки. Він надає аналітичні інструменти для всебічного огляду різних хмарних середовищ, що дає змогу централізовано звітувати та оповіщення.
- Інструменти безперервної інтеграції: вони використовуються для розробки та тестування сценаріїв у межах підходу автоматизації. Зазвичай використовуються такі інструменти, як Ansible і Python, що дає змогу гнучко та ефективно автоматизувати сценарії та оркестрацію.
- Інструмент Orchestrator (наприклад, Rundeck): Rundeck слугує центральним оркестратором, який провадить виділення та управління хмарними ресурсами. Він координує виконання завдань і робочих процесів, визначених у сценаріях автоматизації.
- Управління секретами (наприклад, HashiCorp Vault): цей модуль використовується для безпечного керування та зберігання конфіденційної інформації, як-от паролі, токени та ключі, що важливо для підвищення безпеки хмарних оцінок.
- Інструменти сканування стандартів відповідності та безпеки (наприклад, Prisma Cloud): ці інструменти використовуються для безперервного сканування хмарних конфігурацій на відповідність рекомендованим стандартам кібербезпеки, таким як NIST 800-53, HIPAA, PCIDSS, SOC та ISO, забезпечуючи постійну відповідність.
- Інструменти авдиту та реєстрації потоків: ці інструменти, інтегровані для відстеження та моніторингу операцій і змін у хмарних середовищах, надають потрібні дані для сканування конфігурації та перевірки відповідності.

Список літератури

1. Hashmi Ahtisham & Ranjan Aarushi & Anan Abhineet. (2018). Security and Compliance Management in Cloud Computing. International Journal of Advanced Studies in Computer Science and Engineering (2278-7917). 7. 47–54. Available at: https://www.researchgate.net/publication/323081755_Security_and_Compliance_Management_in_Cloud_Computing

2. Lakhno V., Kozlovskii V., Boiko Y., Mishchenko A., & Opirskyy I. (2017). Management of information protection based on the integrated implementation of decision support systems. Eastern-European Journal of Enterprise Technologies, 5(9 (89), 36–42. DOI: 10.15587/1729-4061.2017.111081

3. Susukailo V., Opirskyy I. and Vasylyshyn S. Analysis of the attack vectors used by threat actors during the pandemic (2020) IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), Zbarazh, Ukraine, 2020, pp. 261–264. DOI: 10.1109/CSIT49958.2020.9321897

4. What is cloud security? Available at: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security

5. Vakhula O., Opirskyy I., Mykhaylova O. Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023) 55–69. Available at: https://ceur-ws.org/Vol-3550/

6. Kalra Sanchi & Atal Kunal & Jain Rachna. (2017). Security Issues in Cloud Computing. International Journal of Computer Applications. 167. 37–41. DOI: 10.5120/ijca2017914190

7. Sreedharan Sherin (2013). Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework. IOSR Journal of Computer Engineering. 10. 33–37. DOI: 10.9790/0661-01043337

8. Sharma Deepak & Dhote Chandrashekhar & Potey Manish. (2013). Security-as-a-Service from Clouds: A Comprehensive Analysis. International Journal of Computer Applications. 67. 15–18. DOI: 10.5120/11374-6642

9. Shevchuk D., Harasymchuk O., Partyka A., Korshun N. Designing Secured Services for Authentication, Authorization, and Accounting of Users, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023) 217–225. Available at: https://ceur-ws.org/Vol-3550/

10. Chirra Prudhvi & Kumar Vineeth. (2023). Multi-cloud networking: investigating strategies and tools for networking in multi-cloud environments. DOI: 10.13140/RG.2.2.11542.93768

11. Inap. (2020, December 15). What are the Differences Between IaaS, PaaS and SaaS? INAP. Available at: https://www.inap.com/blog/iaas-paas-saas-differences/

12. Choi Brendan & Medina Erwin. (2023). Setting Up an Ansible Learning Environment. DOI: 10.1007/978-1-4842-9624-0_4

13. Choi Brendan. (2021). Introduction to Python Network Automation: The First Journey. DOI: 10.1007/978-1-4842-6806-3

14. Sabharwal Navin & Pandey Sarvesh & Pandey Piyush. (2021). Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul: Hands-on Deployment, Configuration, and Best Practices. DOI: 10.1007/978-1-4842-7129-2

15. National Institute of Standards and Technology (NIST). (Latest Update Year). "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations." [Online]. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

16. Edwards K., & Riis J. (2004). Expected and Realized Costs and Benefits from Implementing Product Configuration Systems., 216–231. DOI: 10.4018/978-1-60566-260-2.CH012

17. Dawson John & Twum Frimpong & Acquah James & Missah Yaw. (2023). PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud. Security and Communication Networks. 2023. 1–17. DOI: 10.1155/2023/9210803

18. Catescu Georgeta. (2018). Detecting insider threats using Security Information and Event Management (SIEM). DOI: 10.13140/RG.2.2.11716.99200

19. Spinellis Diomidis. (2014). Service Orchestration with Rundeck. Software, IEEE. 31. 16–18. DOI: 10.1109/MS.2014.92

20. Rajavaram Harika & Rajula Vineet & BalasubramanianThangaraju. (2019). Automation of Microservices Application Deployment Made Easy By Rundeck and Kubernetes. 1–3. DOI: 10.1109/CONECCT47791.2019.9012811

21. HashiCorp. (Latest Update Year). Vault by HashiCorp. [Online]. Available at: https://www.vaultproject.io/

22. Maksymovych V., Shabatura M.; Harasymchuk O., Shevchuk R., Sawicki P., Zajac T. Combined Pseudo-Random Sequence Generator for Cybersecurity. Sensors 2022, 22, 9700. DOI: 10.3390/s22249700

23. Maksymovych V., Nyemkova E., Justice C., Shabatura M., Harasymchuk O., Lakh Y., Rusynko M. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics. (2022); 11(13):2039. DOI: 10.3390/electronics11132039

24. Maksymovych V., Shabatura M., Harasymchuk O., Karpinski M., Jancarczyk D., Sawicki P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. (2022), 12(3), 1519. DOI: 10.3390/app12031519

25. Riti Pierluigi & Flynn David. (2021). Vault HCL. DOI: 10.1007/978-1-4842-6634-2_7

26. ITSM – IT Service Management Solution of your business. Available at: https://www.creatio.com/page/itsm-system

27. Maes Stephane & team, IFS. (2023). ITSM beyond IT. Take the service experience to new heights. IFS. Available at: https://www.researchgate.net/publication/372217278_ITSM_beyond_IT_Take_the_service_experience_to_new_heights

28. What is a REST API? Available at: https://www.redhat.com/en/topics/api/what-is-a-rest-api

29. Williams Brad & Tadlock Justin & Jacoby John. (2020). REST API. DOI: 10.1002/9781119666981.ch12

THE CONCEPT OF AUTOMATED COMPLIANCE VERIFICATION AS THE FOUNDATION OF A FUNDAMENTAL CLOUD SECURITY MODEL

Y. Matseniuk, A. Partyka

Lviv Polytechnic National University,
Information Security Department

The primary objective of this research is to develop an advanced automated method for configuring and managing public cloud accounts and subscriptions on prominent platforms such as AWS, GCP, and Azure. This method involves the application of standardized configurations to ensure optimal performance and security compliance. A significant component of this methodology is the intermittent scanning of the infrastructure of these cloud accounts and subscriptions. This scanning is meticulously designed to identify and address any deviations or non-compliance issues with globally recognized security standards, including NIST 800-53, ISO 27001, HIPAA, and PCIDSS.

The approach leverages cutting-edge automation technologies to streamline the deployment and management of cloud resources. By automating the application of configurations, the method aims to reduce manual effort, minimize the likelihood of human error, and enhance operational efficiency. This automation extends to the continuous monitoring and auditing processes, enabling real-time detection of configuration drifts or security vulnerabilities. Furthermore, the research delves into the development of a dynamic, responsive system capable of adapting to the evolving requirements of cloud security. The automated scanning component plays a pivotal role in this aspect, providing ongoing assurance that the cloud environments adhere to the strictest security protocols and standards.

Continuous compliance monitoring is critical in today's ever-changing digital landscape, where threats to data security and privacy are increasingly sophisticated. By integrating these automated processes, the proposed method promises not only to bolster the security posture of cloud environments but also to offer a scalable, efficient solution for cloud infrastructure management. This automated approach is poised to set a new standard in cloud management, aligning with best practices in IT security and compliance, and paving the way for more secure, manageable, and efficient cloud computing practices.

Keywords: Hosting, security standards, automation, cloud technologies, cloud service models.