УДК 004.4

ІНТЕГРАЦІЯ FINOPS ТА SOC 2-КОНТРОЛІВ У ПРОЦЕС МОНІТОРИНГУ ВИТРАТ У МУЛЬТИХМАРНОМУ СЕРЕДОВИЩІ

Євгеній Марценюк

INTEGRATION OF FINOPS AND SOC 2 CONTROLS INTO THE COST MONITORING PROCESS IN A MULTI-CLOUD ENVIRONMENT

Yevhenii Martseniuk

Національний Університет Львівська Політехніка, м. Львів, Україна

Abstract. *With the growing popularity of multi-cloud architecture, organizations are increasingly facing challenges related to cost opacity, budget overruns, and fragmented control over cloud resource consumption. At the same time, there is a rising demand for compliance with information security standards, particularly SOC 2, which includes criteria for security, availability, and processing integrity (Trust Services Criteria).*

This paper proposes an architectural solution that combines FinOps approaches to cost management with the implementation of SOC 2 controls. Based on tools such as Splunk, Cherwell, and automated event escalation mechanisms, a system was developed that can detect budget overruns, generate incidents, allocate responsibility among process participants, and ensure the logging of all critical events. The implemented logic of thresholds and responses is integrated with the ITSM environment and supports business processes related to financial and security monitoring.

The solution not only enables cost optimization in a multi-cloud environment but also forms an evidence base for audit in accordance with SOC 2 Type II. This demonstrates the effectiveness of an approach that combines economic efficiency, automation, and information security, and can be scaled for medium and large IT organizations.

Проблематика. Стрімке впровадження мультихмарних архітектур у сучасних IT-організаціях супроводжується суттєвими викликами в частині фінансового контролю. Через різнорідність білінгових механізмів у різних хмарних провайдерів (AWS, Azure, GCP), затримки в оновленні даних, фрагментованість джерел та відсутність єдиного аналітичного центру, компанії часто стикаються з перевитратами та неефективним розподілом бюджетів. У таких умовах виникає потреба у створенні централізованих рішень, що не лише оптимізують витрати, але й дозволяють відповідати зовнішнім стандартам інформаційної безпеки, зокрема SOC 2. Цей стандарт виступає не лише як регуляторна вимога, а й як ключовий драйвер впровадження контрольних механізмів у мультихмарному середовищі.

Мета дослідження. Метою дослідження є розробка та обґрунтування архітектурного рішення для моніторингу витрат у мультихмарній інфраструктурі, яке б поєднувало в собі:

- підходи FinOps до управління хмарними витратами;
- автоматизовану логіку реагування на перевитрати на базі платформ Splunk і Cherwell;
- реалізацію контролів відповідно до критеріїв SOC 2, зокрема у сферах безпеки, обробки даних та їх доступності.

Архітектура рішення. У процесі побудови системи моніторингу витрат у мультихмарному середовищі використовуються кілька джерел даних та інструментів. [Рис.1] Основними хмарними платформами, які забезпечують вихідну інформацію про спожиті ресурси, є Google Cloud (GCP), Amazon Web Services (AWS) та Microsoft Azure. Дані про витрати отримуються через API у форматі JSON, який оновлюється тричі на день, що забезпечує майже оперативну актуальність фінансової інформації.

Для подальшої обробки та аналізу даних використовується система Splunk, яка служить центральним елементом моніторингу. Вона отримує інформацію з усіх хмарних провайдерів, порівнює фактичні витрати з встановленими бюджетними лімітами, що зберігаються в системі Cherwell. Остання, у свою чергу, виконує функції управління запитами та фіксації граничних бюджетних показників.

Користувачі взаємодіють із системою через HelpDesk-інтерфейс, який відображає затверджені ліміти на використання хмарних ресурсів. У разі необхідності, через цей же інтерфейс можна подати запит на їх зміну.

Отримані дані аналізуються з точки зору фактичного використання, прогнозуються витрати на наступні періоди та будуються візуалізації у вигляді єдиного інформаційного дашборду. До нього мають доступ лише визначені користувачі відповідно до моделі керування ролями (RBAC), що гарантує захист даних та відповідність політиці доступу.

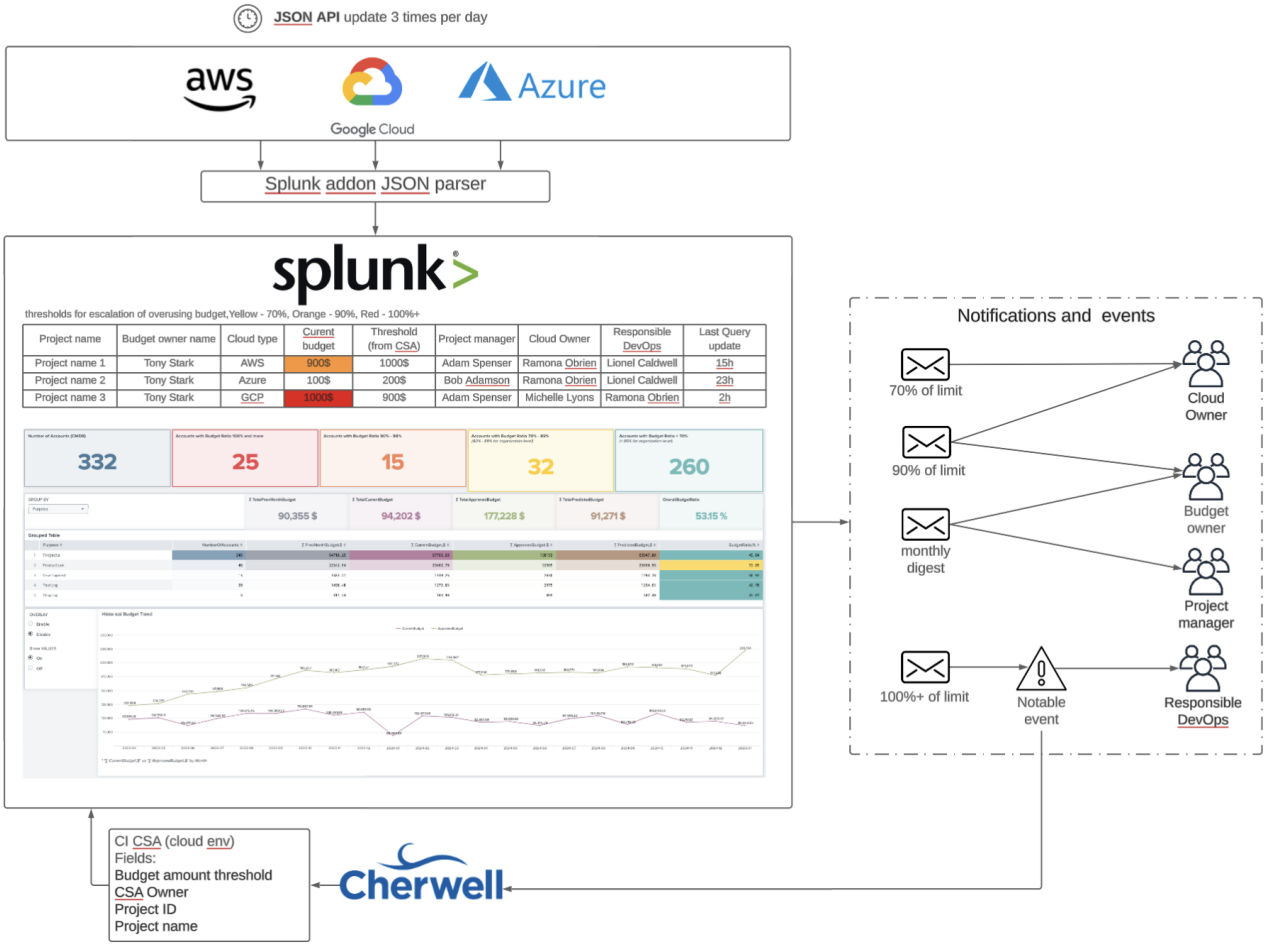

Рисунок 1. Архітектура процесу моніторингу витрат мульти-хмарних середовищ

В системі визначено кілька рівнів порогів витрат, кожен із яких супроводжується відповідними сповіщеннями:

- При досягненні 70% бюджету формується попереджувальне повідомлення, яке надсилається власнику хмарного середовища.
- Коли витрати перевищують 90% від встановленого ліміту, сповіщення отримують як власник середовища, так і відповідальний за бюджет проєкту.
- У разі перевищення бюджету (100% і більше) відбувається ескалація – додатково інформується команда DevSecOps і автоматично створюється інцидент у системі Cherwell.

Кожне повідомлення містить автоматично згенерований прогноз витрат до кінця періоду. Окрім цього, наприкінці місяця проєктні менеджери отримують узагальнений звіт

про стан використання бюджету в усіх хмарних середовищах. Інформація подається у візуальному форматі з використанням кольорової індикації відповідно до рівня споживання ресурсів.

Ця модель дозволяє оперативно виявляти перевитрати бюджету, автоматизувати процеси сповіщення та реагування, а також оптимізувати використання ресурсів, що в кінцевому підсумку сприяє зниженню фінансових ризиків компанії.

Відповідність критеріям SOC 2 (Trust Services Criteria). Запропонована архітектура охоплює такі контрольні області SOC 2:

- **Security** — реалізація доступу за ролями, виявлення аномалій у витратах, запуск захисних сценаріїв;
- **Processing Integrity** — забезпечення точності, повноти й достовірності білінгових даних;
- **Availability** — реакція на події з урахуванням SLA, забезпечення безперервності обслуговування;
- **Monitoring Activities** — логування дій, збереження історії змін, генерація звітів.

Висновки. Результати дослідження підтверджують, що ефективний моніторинг витрат у мультихмарній інфраструктурі є не лише критично важливим для забезпечення фінансової прозорості та раціонального використання ресурсів, а й виступає невіддільною складовою сучасної моделі інформаційної безпеки. Запропоноване рішення дозволяє не лише вирішити ключові проблеми фрагментованості білінгу та затримок в обліку, але й забезпечити реалізацію операційних контролів, які відповідають вимогам стандарту SOC 2.

Архітектура системи інтегрує механізми логування, автоматичного реагування, ескалації інцидентів та відстеження відповідальностей, що узгоджується з критеріями Security, Availability, Processing Integrity та Monitoring Activities у межах Trust Services Criteria (TSC). Використання FinOps-практик у поєднанні з вимогами безпеки дозволяє організації не лише ефективно керувати витратами, а й формувати доказову базу для аудиту, підвищуючи загальний рівень довіри до IT-інфраструктури.

Таким чином, мультихмарна інфраструктура, підкріплена фінансовим та безпековим моніторингом, перетворюється з технічного інструмента на керовану й контрольовану платформу, що відповідає сучасним вимогам до прозорості, стійкості та відповідальності в управлінні цифровими активами.

Бібліографія

1. Kena Alexander, Muhammad Hanif, Choonhwa Lee, Eunsam Kim, Sumi Helal. Cost-aware orchestration of applications over heterogeneous clouds. PLOS ONE, 2020.
2. Liudmyla Shokotko, Anatolii Suprun, Tetiana Petrishyna, Tetiana Pavlysh. Cloud cost monitoring and forecasting: issues and challenges. Economics and Technical Engineering, 2024.
3. Damien T. Wojtowicz, Shaoyi Yin, Jorge Martinez-Gil, Franck Morvan, Abdelkader Hameurlain. Multi-Cloud Query Optimisation with Accurate and Efficient Quoting. IEEE International Conference on Big Data, 2022.
4. Fang Li, Gang Wu, Jianhua Lu, Mingye Jin, Haitao An, Junxiong Lin. SmartCMP: A Cloud Cost Optimization Governance Practice of Smart Cloud Management Platform. IEEE Intl. Conference on Smart Cloud, 2022.
5. Srinivasa Rao Thumala, Binu Sudhakaran Pillai. Cloud Cost Optimization Methodologies for Cloud Migrations. International Journal of Intelligent Systems and Applications in Engineering, 2024.