DOI 10.34185/1562-9945-1-156-2025-04
УДК 004.75:004.42

В.В. Бобренок, А.І. Гуда

АНАЛІЗ OPEN-SOURCE ЗАСОБІВ ДЛЯ ЗАХИСТУ РЕСУРСІВ У ХМАРНИХ СЕРЕДОВИЩАХ

Анотація. Хмарні середовища стають невід'ємною частиною інфраструктури багатьох компаній через свою гнучкість, доступність та ефективність. Проте через свою динамічну природу вони створюють нові загрози безпеці даних, тому потребують окремих засобів для боротьби з ними. У статті проведено порівняння існуючих open source засобів для захисту хмарних середовищ: Checkov, Falco, Keycloak. Розглядаються їх недоліки та переваги, на основі їх аналізу зроблені висновки, що існує потреба у створенні більш досконалих засобів захисту хмарних середовищ.
Ключові слова: хмарні середовища, кібербезпека, програмне забезпечення, open source software, розподілені системи, Checkov, Falco, CSPM, CWPP.

Постановка проблеми

За даними Міжнародної корпорації даних (IDC), глобальний публічні хмарні послуги та інвестиції в інфраструктуру розширилися з 229 мільярдів доларів у 2019 році до 500 мільярдів доларів у 2023 році [1]. Ринок швидко розвивається завдяки збігу факторів: великі підприємства усвідомлюють трансформаційну силу хмарних обчислень, адже завдяки переходу в хмару вони можуть оптимізувати свою інфраструктуру, покращити її стабільність та ефективність, що призводить до підвищення продуктивності всієї організації. Проте зі зростанням популярності хмарних середовищ також відбувається їх постійним розвиток: з'являються нові послуги, вже існуючі оновлюються або замінюються іншими, через що постійно зростає і складність підтримки систем, що використовують ці середовища. Саме ця складність підтримки та розподілена природа подібних систем створюють нові виклики для захисту даних та ресурсів у хмарних середовищах [2]. Так у 2022 середні збитки від витоку даних з хмарних середовищ склали $ 4.35 млн, а кількість загроз зросла на 38% в період з 2022 по 2023 роки [3]. Це робить вибір відповідних засобів для захисту хмарних середовищ важливим кроком для підприємств, що доволі часто обирають програмне забезпечення з відкритим кодом.

Аналіз останніх досліджень і публікацій

У роботі [4] визначено основні виклики у захисті хмарних середовищ та аналізують існуючі методи їх подолання. Зазначано, що існує декілька аспектів, що ускладнюють використання наведених методів:

- інтеграція з існуючою інфраструктурою;
- потреби в додаткових фінансових та людських ресурсах;

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

– відмінності у моніторингу та контролі хмарних середовищ.

Також автори наводять перелік вразливостей, що є найбільш характерними для хмарних середовищ.

Автори [5−6] відзначають важливість систем управління обліковими даними(IAM) у забезпеченні цілісності даних у хмарних середовищах. Проте автори також вказують на складність підтримки подібних систем через постійну потребу в актуалізації даних та необхідність у ретельному контролі прав, що надаються користувачам.

У роботі [7] розглянуто вплив програмного забезпечення з відкритим кодом на галузь кібербезпеки. Одним з висновків є те, що, хоча програмне забезпечення з відкритим кодом робить великий внесок у захист даних та інформаційних систем, воно не є універсальним засобом. Адже різні організації мають різні потреби та обмеження, що можуть унеможливлювати використання подібного програмного забезпечення.

Мета дослідження. Метою дослідження є виявлення їх переваг та недоліків, що дозволяє зробити висновки стосовно поточних тенденцій у сфері захисту хмарних середовищ

Переваги програмного забезпечення з відкритим кодом. Програмне забезпечення з вихідним кодом, доступним для громадськості, відоме як програмне забезпечення з відкритим кодом. Воно надає користувачам можливість змінювати та вдосконалювати вихідний код відповідно до своїх потреб. Таке програмне забезпечення не захищається авторським правом, і користувачі можуть отримати вихідний код і змінити його за потреби. Подібна модель розвитку створює певні переваги, що роблять програмне забезпечення з відкритим кодом привабливим для бізнесу:

– Ціна − більшість програмного забезпечення з відкритим кодом, доступне безкоштовно.

– Швидкість розвитку − проекти з відкритим кодом створюються людьми з різними культурами та точками зору, що працюють на вирішенням спільної проблеми, тому такі проекти доволі часто мають вищу якість, ніж комерційне програмне забезпечення. Нові функції в цих проектах також публікуються часто і швидко завдяки цій груповій стратегії співпраці.

– Стабільність − оскільки над одним проектом працюють тисячі людей, дрібні недоліки швидко усуваються.

– Безпека − відкритість коду дозволяє будь-кому проаналізувати його на потенційні загрози та виправити їх за потреби, що робить подібні додатки безпечнішими у використанні.

Checkov. Checkov − це інструмент, що реалізує CSPM (Cloud Security Posture Management) процес, що дозволяє перевіряти конфігурацію хмарної інфраструктури на поширені проблеми безпеки та відповідності. До таких проблем можуть відноситись незашифровані сегменти зберігання даних, відсутність ключів шифрування або їх ротації. Це дозволяє уникнути наступних ризиків:

– Проблеми відповідності − стандарти відповідності забезпечують оптимальність конфігурацій для підтримки безпеки хмари. Однак розробники можуть не помічати ці стандарти, через що інфраструктура буде вразливою до різноманітних загроз і проблем.

– Порушення безпеки − у хмарній системі можуть бути певні помилки та неправильні конфігурації в коді, якими можуть скористатися зловмисники. Через це можуть виникнути такі проблеми, як викрадення даних, відмова системи.

– Ненавмисні ризики − зазвичай компанії намагаються врахувати навмисні атаки зловмисників на свою систему, але можуть не помічати ненавмисних проблем, таких як вразливість конфіденційних даних. Без інструментів CSPM цей тип ризику неможливо помітити, усунути та вирішити.

– Відсутність розуміння інциденту − через відсутність периметра та централізації порівняно з локальними системами організаціям важко знайти причину інциденту. Отже, вони погано підготовлені для того, щоб зрозуміти, як стався інцидент і його наслідки.

– Серед переваг Checkov можна виділити:

– Допомога в усуненні помилок − при виявленні помилок або загроз безпеці у конфігурації Checkov надає інструкції з їх усунення.

– Інтеграція у CI/CD процеси автоматизує процес виявлення неправильних конфігурацій у хмарі, які можуть призвести до помилок і порушень безпеки в хмарній інфраструктурі компанії.

– Підтримка популярних Infrastructure As Code(IaC) фреймворків

– Пропонує єдину інформаційну точку для різних хмарних середовищ і облікових записів, що дозволяє розробникам у будь-який момент мати видимість того, що відбувається у хмарі.

– Проте CSPM(а отже і Checkov) має свої недоліки, основними серед яких є:

– CSPM не може виправити всі неправильні налаштування − інструменти CSPM зазвичай ефективно виявляють проблеми конфігурації, але вони не завжди можуть виправити неправильну конфігурацію, коли її знаходять, що не дозволяє повністю автоматизувати цей процес.

– Постійний моніторинг неправильних конфігурацій корисний для виявлення проблем відповідності та ризиків, таких як відкриті порти, проблеми з ключами шифрування. Однак проблеми з неправильною конфігурацією становлять лише долю ризиків для безпеки хмарних середовищ. Адже багато кібератак тривають і передбачають складну послідовність подій, а не одноразову аномалію. Інструменти CSPM не відстежують середовище виконання, тому вони не можуть визначити підозрілу поведінку, як-от незрозуміле сплеск активності в мережі.

– Забезпечення відповідності не гарантує безпеки - потреби організації в конфігурації можуть змінюватися, як і вимоги до відповідності, тому команди безпеки та розробки повинні враховувати нові ризики. Інструменти CSPM не надають сповіщень про порушення, які прослизають через існуючі правила.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

– Безпека вимагає комбінованого статико-динамічного підход − інструменти CSPM є статичними за своєю природою — вони відстежують середовище конфігурації під час аналізу на певний момент часу, тому не враховують вплив невеликих змін у часі, які згодом можуть створити загрозу безпеці усієї системи.

– CSPM інструменти іноді можуть генерувати помилкові спрацьовування, що може призвести до втрати часу та ресурсів на розслідування неіснуючих загроз [8].

Falco. Falco − це інструмент, що допомагає реалізувати CWPP (Cloud Workload Protection Platform) процес шляхом всебічного спостереження за додатками та інфраструктурою та аналізу їх продуктивності. Його основними перевагами є:

– Платформа автоматично виявляє загрози та надає засоби для запобігання атакам. Falco може виявити аномалії та відстежувати події в режимі реального часу, що робить його потужним інструментом для забезпечення безпеки.

– Falco допомагає компаніям дотримуватися вимог різних регуляторів, надаючи інструменти для аудиту та створення звітів про безпеку.

– Підтримка AWS, Google Cloud, Azure та інших хмарних служб робить Falco універсальним рішенням для компаній, що працюють у хмарних середовищах.

До недоліків даного інструменту можна віднести:

● Складнощі в інтеграції: Falco потребує встановлення агента для кожного компоненту системи. Враховуючи надзвичайно динамічну, розподілену та ефемерну природу хмари, фактично неможливо встановити агента на кожний компонент системи[9] (не кажучи вже про те, що існує багато ОС, і не всі з них можуть підтримуватися агентами), що може призвести до погіршення якості моніторингу системи в цілому.

– Відсутність інформації про площину керування: Falco охоплює лише робочі навантаження, вони не пропонують жодної інформації про площину керування.

– Неефективна пріоритезація сповіщень: Falco не має доступу до хмари в повному обсязі та не може визначити пріоритетність сповіщень на основі контексту середовища.

– Зловмисники часто намагаються спочатку закріпитися в хмарному середовищі, а потім рухаються до своєї фактичної цілі. Через відсутність уявлення про конфігурації хмари Falco може знаходити аномалії лише в робочих навантаженнях, а не на рівні хмарної інфраструктури, що потенційно залишає відкритими важливі вектори атак.

Keycloak. Keycloak − це open source рішення для ідентифікації користувачів та керування доступом, що вирішує наступні задачі:

– Керування доступом**:** дозволяє керувати доступом до різних додатків та ресурсів, налаштувати політики доступу та ролі користувачів, щоб забезпечити безпечний доступ до даних.

– Автентифікація користувачів: забезпечує безпеку програмних продуктів та даних, оскільки доступ до них буде дозволено тільки авторизованим користувачам.

– Авторизація: Keycloak дозволяє визначати ролі кожного користувача, за допомогою яких стає можливим обмежити доступ користувачів до певних сервісів або даних, що зменшує ризик їх витоку.

До переваг Keycloak можна віднести:

– Безпека відповідно до галузевих стандартів: Keycloak підтримує два основних протоколи – SAML2 і Open ID Connect (OIDC), що забезпечують безпечний і стандартизований зв'язок між різними службами, що спрощує інтеграцію в існуючу інфраструктуру.

– Функції єдиного входу (SSO): Ключовою особливістю Keycloak є можливість єдиного входу, що значно покращує взаємодію з користувачами, адже це дозволяє їм отримати доступ до різних сервісів за допомогою одного набору облікових даних.

– Гнучка інтеграція постачальників ідентифікаційних даних: Keycloak забезпечує легку інтеграцію з кількома постачальниками ідентифікаційних даних (IDP), дозволяючи організаціям використовувати наявну інфраструктуру. Це спрощує автентифікацію користувачів і полегшує керування ідентифікацією користувачів у різних службах.

– Надійні функції безпеки: Keycloak підтримує двофакторну автентифікацію (2FA), включаючи такі методи, як одноразові паролі (OTP), ключі доступу FIDO2 з біометричною автентифікацією та інтеграцією смарт-карт [10].

Незважаючи на всі переваги, Keycloak має суттєві обмеження, що не дозволяє назвати його універсальним інструментом для забезпечення безпеки даних та інфраструктури:

– Масштабованість із високим навантаженням: працювати з Keycloak при високих навантаженнях може бути складно. У таких сценаріях необхідний комплексний аналіз, щоб забезпечити роботу з оптимізації ресурсів.

– Складність налаштування: хоча Keycloak пропонує можливість розширення за допомогою плагінів, інтеграція з деякими системами може потребувати значних ресурсів. Крім того, подібні інтеграції можуть мати ненавмисні або пізно виявлені впливи на продуктивність і безпеку.

– Вразливість до компрометування облікових даних: якщо зловмисники отримають доступ до облікових даних одного з користувачів, це наражає систему на небезпеку, адже може пройти доволі багато часу перш ніж це буде виявлено.

Висновки

В роботі розглянуті популярні open source інструменти для захисту хмарних середовищ. Приведені їх особливості, переваги та недоліки. Як можна побачити, існує велика кількість програмного забезпечення з відкритим кодом, що може бути використано для захисту даних та інфраструктури у хмарних середовищах. Проте кожне з наведених рішень має свої недоліки, що робить їх вразливими для певних видів атак та не дозволяє назвати їх універсальними. Через це виникає потреба в розгортанні та підтримці одразу декількох інструментів, що призводить до ускладнення систем в цілому та збільшує витрати на них. Також ускладнення системи може створити нові неочевидні вектори атак. Це демонструє потребу у створенні більш досконалих та універсальних засобів, що зможуть спростити процес захисту хмарних середовищ.

ЛІТЕРАТУРА

1. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Computer Science Review, vol. 33, pp. 1–48, 2019.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

2. Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail –Joon and Ahn Arizona State University, “Security and Privacy Challenges in Cloud Computing Environments”, IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31
3. The Latest 2024 Cyber Crime Statistics [Електронний ресурс] - 2024. - Режим доступу до ресурсу: https://aag-it.com/the-latest-cyber-crime-statistics/
4. Chauhan, Milan & Shiaeles, Stavros. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 3. 422-450. 10.3390/network3030018.
5. Mogos, Gabriela. (2019). Cloud Security. Critical analysis. International Journal of Computer Science and Information Security,. 17. 51-54.
6. Singh, Chetanpal & Thakkar, Rahul & Warraich, Jatinder. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 8. 30-38. 10.24018/ejeng.2023.8.4.3074.
7. Doinea, Mihai. (2010). Open Source Security Tools. Open Source Science Journal. 2.
8. International Journal of Scientific Research in Computer Science, E., & IJSRCSEIT, I. T. (2020). CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/CSEIT206268
9. Yadav, Baleshwar & Sharma, Mansi. (2023). Cloud Workload Protection Platform Market.
10. D., Divyabharathi & Cholli, Nagaraj. (2020). A Review on Identity and Access Management Server (KeyCloak). International Journal of Security and Privacy in Pervasive Computing. 12. 46-53. 10.4018/IJSPPC.2020070104.

REFERENCES

1. R. Kumar and R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,” Computer Science Review, vol. 33, pp. 1–48, 2019.
2. Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail –Joon and Ahn Arizona State University, “Security and Privacy Challenges in Cloud Computing Environments”, IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31
3. The Latest 2024 Cyber Crime Statistics [Електронний ресурс] - 2024. - Режим доступу до ресурсу: https://aag-it.com/the-latest-cyber-crime-statistics/
4. Chauhan, Milan & Shiaeles, Stavros. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 3. 422-450. 10.3390/network3030018.
5. Mogos, Gabriela. (2019). Cloud Security. Critical analysis. International Journal of Computer Science and Information Security,. 17. 51-54.
6. Singh, Chetanpal & Thakkar, Rahul & Warraich, Jatinder. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 8. 30-38. 10.24018/ejeng.2023.8.4.3074.
7. Doinea, Mihai. (2010). Open Source Security Tools. Open Source Science Journal. 2.
8. International Journal of Scientific Research in Computer Science, E., & IJSRCSEIT, I. T. (2020). CSPM- Cloud Security Posture Management (Comprehensive Security for Cloud Environment). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/CSEIT206268
9. Yadav, Baleshwar & Sharma, Mansi. (2023). Cloud Workload Protection Platform Market.

10. D., Divyabharathi & Cholli, Nagaraj. (2020). A Review on Identity and Access Management Server (KeyCloak). International Journal of Security and Privacy in Pervasive Computing. 12. 46-53. 10.4018/IJSPPC.2020070104.

Received 13.01.2025.
Accepted 16.01.2025.

Analysis of open-source tools for protecting resources in cloud environments

Cloud environments are becoming an integral part of the infrastructure of many companies due to their flexibility, accessibility and efficiency. However, due to their dynamic nature, they create new threats to data security, therefore, they require separate tools to combat them. The article compares existing open source tools for protecting cloud environments: Checkov, Falco, Keycloak. According to the article, the main benefits of open source software are: price, stability and community support.

For each of the tools some flaws are found which make these tools vulnerable to malicious actors:

– Checkov implements CSPM process which does not monitor the runtime environment, so it cannot identify suspicious behavior, such as an unexplained spike in network activity.

– Falco is hard to integrate into existing systems as it requires agents to be added to each component. Also it does not has any information on the control pane so it does not view on the entirety of the cloud which allows attacks to target underlying infrastructure instead of workloads

– Keycloak has issues with scalability and can be difficult to configure and customize to integrate with some systems. Some systems might require some custom solutions to make integration possible and these solutions can lead to new vulnerabilities being introduced into the system. Also clients' credentials might get compromised which can allow bad actors to access the system.

These flaws make these tools not universal, so it creates the need to deploy and support several tools at once to protect the cloud, which leads to the complexity of the systems as a whole and increases their costs. Also, the complexity of the system can create new, non-obvious attack vectors. This demonstrates the need to create more advanced and universal tools that can simplify the process of protecting cloud environments.

Keywords: cloud environments, cybersecurity, software, open source software, distributed systems, Checkov, Falco, CSPM, CWPP.

Бобренок Вячеслав Віталійович - аспірант кафедри інформаційних технологій і систем Українського державного університету науки і технологій.
Гуда Антон Ігорович - доктор технічних наук, професор кафедри інформаційних технологій і систем Українського державного університету науки і технологій.

Bobrenok Viacheslav - Post graduate student of the Department of Information Technologies and Systems of the Ukrainian State University of Science and Technology
Guda Anton - Doctor of Technical Sciences, Professor of the Department of Information Technologies and Systems of the Ukrainian State University of Science and Technology.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)