

---

**Шкоденко Тарас Володимирович**  
магістр економічної кібернетики, аспірант денної форми навчання  
*КНЕУ ім.Вадима Гетьмана, Україна*

---

## ПРО ОДИН ІЗ АСПЕКТІВ ЗАХИСТУ ДАНИХ У БІЗНЕСІ

### **Вступ**

В сучасних умовах економіки при веденні бізнесу набуває особливої актуальності питання захисту бізнес інформації. Особливо гостро це питання постає в аспекті захисту великих даних. Більшість сучасних рішень електронної комерції використовують в якості систем для хостингу Cloud-based [6] площадки такі як: Amazon AWS, Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud Infrastructure та VMWare Tanzu. Такі задачі як: постійний аналіз, моніторинг та виправлення загроз безпеки всіх серверів подібної Cloud інфраструктури [6] може бути надзвичайно складним, або навіть не можливим для ефективного виконання навіть групою ІТ спеціалістів. Щоб забезпечити тим самим стабільну та безперебійну роботу систем подібної складності, що в ідеалі мають працювати 24 години 7 днів на тиждень 365 днів на рік із показниками доступності всієї архітектури серверів з uptime 99,9%.

### **Основна частина**

Одним із найкращих доступних на сьогоднішній день рішень, які є в наявності, здатних допомогти ІТ спеціалістам у вирішенні широкого спектру задач забезпечення безпеки для рішень інфраструктури серверів електронного бізнесу включаючи захист великих даних є SAAS-платформа [8] Sysdig Secure [1]. Вона дозволяє в режимі реального часу моніторити наявні загрози безпеки, допомагає виправляти їх, а також сканувати в автоматичному режимі програмний код та інтегруватися з багатьма популярними сучасними системами Infrastructure as Code (IaC) [2]. Що є складовою більш складної та популярної в наші дні концепцією DevOps toolchain [3].

Розглянемо детальний перелік можливостей платформи Sysdig Secure:

- Компонент для підвищення безпеки у Infrastructure as Code (IaC) [4], що дозволяє ефективно керувати ризиками конфігурацій у хмарі за допомогою інструменту безпеки Infrastructure as Code (IaC) Security, що вбудований в Sysdig Secure та дозволяє застосовувати узгоджену політику безпеки для багатьох середовищ Infrastructure as Code (IaC), хмарних середовищ хостингу [6] та екосистеми Kubernetes [5]. Автоматичні виявлення та виправлення загроз, закриття питань забезпечення надійного захисту повного циклу: від конфігурації інфраструктури у продакшен середовищі до джерела програмного коду.
- Компонент Cloud Security Posture Management (CSPM) дозволяє позначати неправильні конфігурації та постійно відстежувате підозрілу активність за допомогою CSPM [7] в середовищі SaaS платформи [8] Sysdig Secure. Компонент дозволяє ефективно виконувати наступні завдання:
  - Запобігання дрейфу. Скануйте файли IaC [4] перед розгортанням. Зіставляти неправильні конфігурації у продакшені та повертатися назад до джерела програмного коду, що використовується.
  - Пріоретизувати можливі ризики. Визначайте самостійно пріоритетність наявних виправлень безпеки на основі контексту програми, усіх можливих істотних вимог і також залежностей.
  - Виправлення у джерела. Отримуйте корисні рекомендації щодо виправлення у джерела за допомогою автоматично створених запитів на отримання.

- Компонент для керування правами хмарної інфраструктури (CIEM) [9]. Дозволяє користувачам отримати поліпшену видимість усіх наявних хмарних облікових записів, керувати всіма наявними дозволами користувачів платформи Sysdig Secure.
- Компонент контролю відповідності набору правил безпеки у Хмарному середовищі Cloud Security Compliance [10] дозволяє користувачам дотримуватись суворих та чітких стандартів відповідності (PCI, NIST, GDPR тощо) для контейнерів і хмарного середовища в цілому. Що включає в себе такі елементи як:
  - Підтвердження відповідності. Ви можете використати вже готові працюючі засоби керування, що дозволить відносно легко дотримуватись відповідності всім існуючим нормативним стандартам (PCI, NIST, GDPR тощо) для вашого хмарного середовища загалом та усіх контейнерів з яких воно складається протягом усього життєвого циклу програми.
  - Увімкніть автоматизацію. Усуньте не надійні ручні процеси та забезпечте відповідність елементам керування за допомогою політики як коду на основі OPA [20].
  - Автоматичне проходження аудитів. Продемонструйте як доказ відповідності вашого хмарного середовища та контейнерів за допомогою журналів аудиту хмари та даних аналітики з контейнерів.
- Компонент для сканування вразливостей контейнерів Container Vulnerability Scanning [11] дозволяє визначати пріоритетність найбільш критичних уразливостей, використовуючи контекст виконання. Автоматизуйте конвеєр CI/CD [12] і сканування реєстру та блокуйте вразливості коду перед їх виходом у продакшен.
- Компонент хмарного виявлення та реагування у відповідь Cloud Detection & Response (CDR) дозволяє виявляти та відповідно реагувати на виникаючі загрози в контейнерах, хостах, Kubernetes [5] і хмарі на основі відкритого коду Falco [14]. Він складається з таких елементів:
  - Виявлення робочого навантаження та відповідь. Безпечне середовище виконання в контейнерах, без серверів і Kubernetes [5]. Що дозволить вам виявляти загрози за допомогою керованих політик і ML. Автоматично відповідайте діями та з детальною експертизою.
  - Хмарний моніторинг безпеки. Дозволяє користувачам виявляти зміни в конфігурації, аналізуючи журнали аудиту активності в хмарі (AWS CloudTrail, журнали аудиту Google Cloud Platform, журнали активності Azure) за допомогою Falco [14].
  - EDR хоста/сервера. Виявляйте аномальну активність і загрози всередині хостів і віртуальних машин (VM) [15] за допомогою політик на основі Falco [14].
  - Багаторівневе виявлення загроз
    - Виявлення на основі ML [16]. Блокуйте криптомайнери з точністю 99% за допомогою виявлення на основі машинного навчання (ML) [16]. Виявляйте аномалії (системні виклики, активність мережі, процесів і файлів) за допомогою профілювання поведінки на основі ML [16].
    - Запобігання дрейфу контейнерів. Блокувати виконання файлів, яких не було в оригінальному контейнері. Зупиніть зловмисне програмне забезпечення, зловмисних користувачів і ризиковану застарілу практику, застосувавши принципи хмарної незмінності.
    - Багаторівневе виявлення загроз. Виявляйте загрози в контейнерах, Kubernetes [5] і хмарі на основі Falco [14]. Блокуйте атаки за допомогою контролю дрейфу та загроз, що надходять із спеціальних інформаційних каналів у автоматичному режимі. Збільшуйте охоплення за допомогою вже готових політик, зібраних та керованих командою дослідження загроз від Sysdig.
    - Реагуйте на інциденти та запобігайте втручанню криміналу. Фіксуйте детальну діяльність усіх користувачів та систем, включаючи команди, мережеві підключення та дії з

файлами. Збагачайте події за допомогою метаданих контейнера, Kubernetes або хмари. Легко пересилайте події до інструментів SIEM [17].

- Компонент безпеки мереж Kubernetes [5] (Kubernetes Network Security) [18]. Дозволяє користувачам захистити мережі Kubernetes [5] за допомогою автоматичної мікросегментації. Переглядайте та перевіряйте всі комунікації між модулями, службами та програмами. Він містить наступні функціональні особливості:

- Моніторинг мережі Kubernetes [5]. Дозволяє користувачам переглядати всю мережеву активність у певному модулі, службі чи програмі та поза ними. Розслідуйте підозрілий трафік і спроби підключення.

- Kubernetes-власна мікросегментація. Увімкніть мікросегментацію за допомогою хмарних мережевих політик Kubernetes [5] із багатим контекстом. Застосуйте безпеку мережі Kubernetes [5], не порушуючи програму.

- Автоматизовані мережеві політики. Значної економії часу можливо досягти за допомогою автоматизації мережевих політик Kubernetes [5]. Використовуйте простий графічний інтерфейс програмного забезпечення, щоб змінювати політики без зміни YAML [19] конфігурації вручну.

- Компонент системи контейнерної експертизи та реагування на інциденти (Container Forensics and Incident Response) [21]. Оптимізуйте реагування на інциденти в контейнерах, Kubernetes [5] і без серверів, а також проводьте криміналістику навіть після того, як контейнери вже зникнуть.

### Висновки

Сучасні технології створюють виклики щодо забезпечення достатньо високого рівня безпеки при веденні економічної діяльності. Особливо у середовищі великих даних підприємств. Подібні виклики вимагають відповідної реакції, яка може бути забезпечена при умові використання програмного забезпечення з функціоналом, що є в програмному засобі Sysdig Secure [1]. Саме тому, його використання є надзвичайно зручним та доцільним для підприємств та при веденні електронного бізнесу пов'язаного з великими даними (Bigdata).

### Список використаних джерел:

1. Sysdig Secure — Sysdig [Електронний ресурс] — Режим доступу : <https://sysdig.com/products/secure/>
2. Infrastructure as code (IaC) — [Електронний ресурс] — Режим доступу : [https://en.wikipedia.org/wiki/Infrastructure\\_as\\_code#:~:text=Infrastructure%20as%20code%20\(IaC\)%20is,configuration%20or%20interactive%20configuration%20tools.](https://en.wikipedia.org/wiki/Infrastructure_as_code#:~:text=Infrastructure%20as%20code%20(IaC)%20is,configuration%20or%20interactive%20configuration%20tools.)
3. DevOps toolchain — [Електронний ресурс] — Режим доступу : [https://en.wikipedia.org/wiki/DevOps\\_toolchain](https://en.wikipedia.org/wiki/DevOps_toolchain)
4. Infrastructure as Code (IaC) Security — [Електронний ресурс] — Режим доступу : <https://sysdig.com/use-cases/infrastructure-as-code-security/>
5. Overview | Kubernetes — [Електронний ресурс] — Режим доступу : <https://kubernetes.io/docs/concepts/overview/>
6. What is cloud hosting? — [Електронний ресурс] — Режим доступу : <https://www.ibm.com/cloud/learn/what-is-cloud-hosting>
7. Cloud Security Posture Management (CSPM) — [Електронний ресурс] — Режим доступу : <https://sysdig.com/use-cases/cspm/>
8. Програмне забезпечення як послуга (англ. Software as a service, SaaS) — [Електронний ресурс] — Режим доступу : [https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5\\_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F\\_%D1%8F%D0%BA\\_%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F_%D1%8F%D0%BA_%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3%D0%B0)
9. Cloud Infrastructure Entitlement Management (CIEM) — [Електронний ресурс] — Режим доступу: <https://sysdig.com/use-cases/cspm/permissions-entitlement-management/>

10. Cloud Security Compliance — [Электронный ресурс] — Режим доступа : <https://sysdig.com/use-cases/compliance/>
11. Container Vulnerability Scanning — [Электронный ресурс] — Режим доступа : <https://sysdig.com/use-cases/vulnerability-management/>
12. CI/CD — [Электронный ресурс] — Режим доступа : <https://en.wikipedia.org/wiki/CI/CD>
13. Cloud Detection & Response (CDR) — [Электронный ресурс] — Режим доступа : <https://sysdig.com/use-cases/cloud-threat-detection-and-response/>
14. Threat Detection Built on Falco — [Электронный ресурс] — Режим доступа : <https://sysdig.com/opensource/falco/>
15. Virtual machine — [Электронный ресурс] — Режим доступа : [https://en.wikipedia.org/wiki/Virtual\\_machine](https://en.wikipedia.org/wiki/Virtual_machine)
16. Machine learning — [Электронный ресурс] — Режим доступа : [https://en.wikipedia.org/wiki/Machine\\_learning](https://en.wikipedia.org/wiki/Machine_learning)
17. Security information and event management (SIEM) — [Электронный ресурс] — Режим доступа : [https://en.wikipedia.org/wiki/Security\\_information\\_and\\_event\\_management](https://en.wikipedia.org/wiki/Security_information_and_event_management)
18. Kubernetes Network Security — [Электронный ресурс] — Режим доступа : <https://sysdig.com/use-cases/kubernetes-network-security/>
19. YAML — [Электронный ресурс] — Режим доступа : <https://en.wikipedia.org/wiki/YAML>
20. Oracle Intelligent Advisor (also known as Oracle Policy Automation) — [Электронный ресурс] — Режим доступа : [https://en.wikipedia.org/wiki/Oracle\\_Intelligent\\_Advisor](https://en.wikipedia.org/wiki/Oracle_Intelligent_Advisor)
21. Container Forensics and Incident Response — [Электронный ресурс] — Режим доступа : <https://sysdig.com/use-cases/container-forensics/>