Vol. 7, No. 2, 2025

DOI: https://doi.org/10.23939/csn2025.02.177

УДК 004.75; 004.8

АВТОМАТИЗАЦІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ В ХМАРІ НА ОСНОВІ SOAR-ПІДХОДУ

О. С. Сапсай, Є. В. Марценюк, А. І. Партика

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: oksana.sapsai.kb.2022@lpnu.ua, yevhenii.v.martseniuk@lpnu.ua, andrii.i.partyka@lpnu.ua

Сучасні організації дедалі частіше інтегрують публічні хмарні платформи, такі як AWS, Azure та Google Cloud Platform, у свою інфраструктуру з метою підвищення гнучкості та масштабованості. Однак мультихмарні середовища породжують нові виклики для кібербезпеки. Людський фактор і недбале поводження з параметрами доступу до хмарних ресурсів можуть призвести до серйозних загроз. Зокрема, якщо зловмисник отримує доступ до ключів авторизації, він може не лише контролювати наявні ресурси, але й створювати нові у власних цілях – для проведення атак, розповсюдження шкідливого програмного забезпечення або майнінгу криптовалют. Такі інциденти можуть швидко спричинити фінансові втрати, підірвати довіру користувачів і вплинути на стабільність критичних сервісів.

У цьому дослідженні розглянуто використання Splunk SOAR (Security Orchestration, Automation, and Response) як інструменту для автоматичного виявлення, аналізу та реагування на загрози у публічних хмарних середовищах. Основна увага зосереджена на інтеграції Splunk SOAR із API хмарних провайдерів для динамічного блокування скомпрометованих ресурсів та реалізації детальних сценаріїв реагування (playbook), що дають змогу ізолювати загрози на рівні окремих компонентів (віртуальні машини, мережеві політики, облікові записи користувачів).

Також проаналізовано інтеграцію Splunk для виявлення аномалій через Palo Alto Prisma як комплексний сканер відхилень, використання HashiCorp Vault для захисту облікових даних, впровадження режиму карантину для ізоляції скомпрометованих ресурсів та вдосконалення процесів реагування на інциденти.

Результати дослідження показують, що автоматизація процесів безпеки за допомогою Splunk SOAR суттєво скорочує час реагування, мінімізує вплив людського фактора та знижує ризик компрометації хмарної інфраструктури. Запропонований підхід підвищує стійкість організації до загроз у мультихмарному середовищі, забезпечуючи оптимальний баланс між безпекою, доступністю та ефективністю роботи.

Ключові слова: хмарна безпека, публічні хмарні середовища, мультихмарна інфраструктура, Splunk SOAR, автоматизоване реагування на інциденти, управління інцидентами, усунення загроз, блокування ресурсів, моніторинг аномалій, API хмарних провайдерів, операції безпеки, автоматизація, DevOps, розвідка загроз, людський фактор.

Вступ

Зростання популярності публічних хмарних платформ, таких як AWS, Azure і Google Cloud Platform, суттєво трансформувало сучасну IT-інфраструктуру, забезпечивши організаціям гнучкість, масштабованість та економічну ефективність. Водночас цей перехід супроводжується новими

викликами у сфері безпеки, особливо у мультихмарному середовищі, де управління доступом, моніторинг загроз і реагування на інциденти стають дедалі складнішими. Одним із ключових ризиків є людський фактор та неналежне поводження з обліковими даними доступу до хмари. У разі, якщо зловмисники отримають несанкціонований доступ до ключів автентифікації, вони можуть використати хмарне середовище для створення та керування ресурсами з шкідливою метою – включно з витоками даних, поширенням шкідливого ПЗ чи майнінгом криптовалют [1].

Традиційні підходи до реагування на інциденти безпеки в хмарі часто передбачають ручне втручання, що може призводити до затримок у реагуванні, неефективного стримування загроз і високих операційних витрат. Крім того, організації стикаються з такими проблемами, як велика кількість хибнопозитивних сповіщень, відсутність деталізованих засобів нейтралізації загроз і низька координація між командами безпеки. Усе це засвідчує необхідність у впровадженні автоматизованого, масштабованого та інтелектуального рішення для виявлення, аналізу та реагування на інциденти безпеки в реальному часі.

Метою цього дослідження є створення комплексної архітектури автоматизованого реагування на інциденти безпеки (SOAR) у мультихмарному середовищі, яка забезпечує динамічне управління секретами, контрольоване втручання в інфраструктуру та масштабованість до середовищ із понад 400 хмарними обліковими сутностями без централізованого адміністрування. Дослідження спрямоване на формалізацію логіки перетворення аномалій на керовані зміни в інфраструктурі з перевіркою авторизації на кожному етапі та побудову моделі оцінки ризиків із кількісними метриками впливу, зокрема економічною оцінкою. Крім того, ставиться за мету впровадити принципи Zero Trust, UEBA та аналітику машинного навчання у процес ухвалення рішень, а також реалізувати самонавчальний механізм для адаптивного оновлення політик реагування на основі накопиченого досвіду – без необхідності ручного втручання.

Наукова гіпотеза полягає у тому, що інтеграція інструментів оркестрації, автоматизації, аналітики та контролю доступу дає змогу створити універсальну модель автоматизованого реагування, здатну забезпечити своєчасну нейтралізацію інцидентів і зменшення пов’язаних із ними фінансових ризиків. Наукове питання, яке постає в межах дослідження: якою мірою використання моделі SOAR з елементами Zero Trust і UEBA здатне покращити ефективність реагування на інциденти в мультихмарному середовищі?

Огляд літературних джерел

Низка досліджень присвячена вивченню викликів і рішень у сфері хмарної безпеки та автоматизованого реагування на інциденти. Наприклад, праці [1–2] акцентують увагу на зростаючій ролі автоматизації в галузі кібербезпеки, особливо в контексті динамічних і масштабованих хмарних середовищ.

Концепція SOAR сформувалась як відповідь на необхідність зменшення ручного втручання та підвищення ефективності центрів операцій безпеки (SOC). Згідно з даними Suram [3], автоматизація управління ідентичностями та доступом (IAM) відіграє критично важливу роль у захисті хмарних платформ. Аналогічно Thokala [6] підкреслює значення масштабованого розгортання хмарної інфраструктури та оркестрації для забезпечення безпеки в системах електронної комерції.

Останні дослідження [4–5] аналізують ризики Shadow IT і централізованого управління секретами, підкреслюючи необхідність використання інтегрованих інструментів оркестрації, таких як SOAR. Ці результати узгоджуються з практиками провідних компаній, де Splunk SOAR і Prisma Cloud використовуються для виявлення, класифікації та реагування на загрози в публічних хмарних середовищах.

Крім того, Soldatenko і Vik [7] досліджували застосування інфраструктури як сервісу (IaaS) і підкреслювали операційні переваги автоматизації в безпеці хмарної інфраструктури. В інших працях [8–10] висвітлено взаємодію штучного інтелекту, хмарних пайплайнів та автоматизації на основі блокчейну, що вказує на перспективні напрями для подальшого вдосконалення систем управління хмарною безпекою.

Постановка задачі

Це дослідження присвячене застосуванню підходу SOAR (Security Orchestration, Automation, and Response) як комплексного рішення для автоматизації управління інцидентами безпеки в публічному хмарному середовищі. Основна увага зосереджена на інтеграції Palo Alto Prisma з API хмарних провайдерів для динамічного виявлення та ізоляції скомпрометованих ресурсів за допомогою автоматизованих сценаріїв. Ключовими компонентами рішення є:

- моніторинг аномалій через Palo Alto Prisma для виявлення підозрілої активності в хмарному середовищі;
- автоматизовані механізми карантину (Quarantine Mode), які запобігають порушенням безпеки з мінімальним впливом на операції;
- інтеграція з HashiCorp Vault для захисту облікових даних і запобігання несанкціонованій ескалації привілеїв;
- гранульоване блокування ресурсів, що дає змогу локалізувати загрози без зупинки всієї хмарної інфраструктури;
- процедури післяінцидентного аналізу для постійного вдосконалення безпеки та адаптивного реагування.

Результати дослідження показують, що впровадження автоматизованого реагування на інциденти за допомогою SOAR значно підвищує рівень безпеки в хмарному середовищі завдяки скороченню часу реагування, зменшенню впливу людського фактора та забезпеченню ефективної ізоляції ресурсів. Використання структурованих механізмів реагування та автоматизації дає змогу організаціям ефективно нейтралізовувати загрози під час збереження стійкості й доступності хмарної інфраструктури [2].

Наукова новизна цього дослідження полягає у розробці та практичному впровадженні багаторівневої архітектури автоматизованого реагування на інциденти безпеки в публічних хмарних середовищах. Запропонована модель інтегрує Splunk SOAR, Jenkins і HashiCorp Vault, формуючи єдину систему управління інцидентами. Вперше представлено динамічно активований сценарій автоматизації “RedButton” для команд L2 SecOps, що забезпечує оркестрацію ізоляції ресурсів у реальному часі в середовищах AWS, Azure та GCP. Такий підхід дає змогу поєднати швидкість реагування, безпеку та операційну безперервність, одночасно зменшуючи ризики несанкціонованого доступу та затримки усунення інцидентів.

Основні розділи дослідження

У контексті забезпечення інформаційної безпеки в публічних хмарних середовищах ключовим завданням є систематична ідентифікація та оцінка ризиків, які можуть призвести до компрометації даних або порушення цілісності інфраструктури. Зважаючи на складність мультихмарних середовищ і високу динаміку змін у них, особливу актуальність набуває аналіз загроз, пов’язаних із несанкціонованим доступом, слабкими механізмами автентифікації та недостатньою сегментацією середовища [6].

1. Оцінка ризиків і роль SOAR у їх мінімізації

У дослідженні застосовано методологію оцінки ризиків, визначену стандартом NIST SP 800-30, яка ґрунтується на якісному аналізі загроз із використанням двох основних параметрів: імовірності виникнення та потенційного впливу. Такий підхід дав змогу побудувати матрицю критичності ризиків, яку подано у табл. 1. Визначені ризики були ранжовані за рівнем критичності, що створює основу для формування ефективної стратегії реагування та розробки надійних механізмів безпеки в умовах мультихмарної інфраструктури [13].

Рішення SOAR відіграє ключову роль у мінімізації ризиків, пов’язаних із безпекою публічних хмарних середовищ, забезпечуючи автоматизовану, швидку та узгоджену реакцію на загрози. Його застосування суттєво скорочує час між виявленням ризику та впровадженням заходів реагування, що є критично важливим у випадках несанкціонованого доступу або експлуатації вразливостей [7].

Завдяки інтеграції з системами моніторингу безпеки, платформами керування обліковими даними та інструментами автоматизації інфраструктури SOAR створює уніфіковану структуру реагування, здатну оперативно нейтралізувати загрози та ізолювати потенційно скомпрометовані ресурси [9].

Таблиця 1

Поширені сценарії інцидентів у публічних хмарних середовищах та їхнє покриття моделлю SOAR

№	Сценарій вторгнення	Первинна вразливість	Ймовірність	Вплив	Рівень ризику	Реакція моделі SOAR
1	Атакуючий отримує доступ до облікового запису розробника через витік облікових даних у публічному репозиторії	Відсутність MFA; слабкий захист секретів	Висока	Високий	Критичний	Виявлення аномального входу; автоматичне блокування акаунту; ініціація ротації секретів через Vault
2	Зловмисник створює нові привілейовані ресурси (EC2, IAM політики) після компрометації користувача	Відсутність моделі Zero Trust; неефективний контроль дій користувачів	Висока	Середній	Високий	Моніторинг змін ресурсів; виконання плейбуків для блокування та ізоляції створених сутностей
3	Після початкового доступу зловмисник здійснює латеральний рух між VPC/проєктами для розширення привілеїв	Відсутність сегментації мережі; неізольовані ролі; спільні токени	Середня	Високий	Високий	Сегментація трафіку; ізоляція регіонів; аудит та обмеження прав доступу; автоматизована реакція SOAR
4	Встановлення бекдору через доступ до функцій (Lambda, GCF) або S3-бакетів із подальшою ексфільтрацією даних	Неналежна політика доступу; анонімний доступ до об’єктів; неаудитовані API	Середня	Високий	Високий	Виявлення сплесків API-запитів; обмеження доступу; карантин об’єктів; сповіщення SecOps
5	Ресурси (наприклад, обчислювальні інстанси) використовуються для майнінгу криптовалют або участі в ботнеті	Необмежений вихідний трафік; слабкий моніторинг активності	Висока	Середній	Високий	Виявлення аномального навантаження; призупинення ресурсів; інтеграція з Jenkins для відкату до базового стану

Крім того, SOAR зменшує вплив людського фактора у процесі реагування, що знижує ймовірність помилок або затримок у прийнятті рішень під час інцидентів [5]. Інтеграція принципів Zero Trust та аналітики поведінки користувачів і сутностей (UEBA) у межах SOAR дає змогу проактивно виявляти аномалії та потенційно зловмисну активність ще до того, як загроза ескалюється [10]. Додатковою перевагою є використання механізмів машинного навчання, які забезпечують здатність системи до самонавчання на основі попередніх інцидентів. Це сприяє постійній адаптації сценаріїв захисту до нових типів загроз, підвищуючи ефективність захисту в умовах динамічного середовища [4].

Отож впровадження SOAR сприяє формуванню проактивної та адаптивної системи інформаційної безпеки, яка не лише знижує ймовірність реалізації ризиків, а й пом'якшує наслідки інцидентів у разі їх виникнення, забезпечуючи відповідність сучасним стандартам захисту інформації [12].

2. Уразливості хмарної інфраструктури за відсутності моніторингу

Використання публічних хмарних сервісів без впровадження комплексних засобів моніторингу та автоматизованого контролю створює значні передумови для порушення базових атрибутів інформаційної безпеки – конфіденційності, цілісності та доступності даних. Відсутність безперервного спостереження за аномальною активністю, обмеженість механізмів кореляції подій та недостатній контроль процесів автентифікації й авторизації суттєво підвищують імовірність тривалого непоміченого перебування зловмисників у хмарному середовищі (dwell time), що ускладнює своєчасне виявлення інцидентів і затримує реалізацію заходів реагування. Така ситуація призводить до зростання ризику не лише локального компрометування ресурсів, а й ескалації доступу, поширення загроз та виникнення каскадного впливу на суміжні інформаційні системи. Крім того, відсутність централізованого моніторингу обмежує можливості організацій щодо виявлення порушень політик безпеки, фіксації аномальної поведінки користувачів і запобігання несанкціонованому використанню API, що набуває особливої критичності в умовах мультихмарної інфраструктури зі складною топологією та численними точками доступу.

3. Засоби виявлення загроз та автоматизовані системи реагування як основа стратегії безпеки хмарної інфраструктури

Ефективна стратегія забезпечення інформаційної безпеки в публічних хмарних середовищах потребує інтеграції двох ключових компонентів: засобів виявлення загроз та систем оркестрації, автоматизації і реагування на інциденти безпеки (SOAR). Такий подвійний підхід дає змогу не лише здійснювати всебічний моніторинг стану хмарної інфраструктури в реальному часі, а й формувати адаптивні реакції на широкий спектр загроз з урахуванням їхньої природи, критичності та потенційного впливу на активи організації [2].

Засоби виявлення загроз здійснюють глибоку перевірку телеметрії хмарного середовища, використовуючи аналіз поведінкових шаблонів, виявлення аномалій, кореляцію подій та джерела аналітики загроз (threat intelligence feeds). Їхня роль полягає в ідентифікації потенційних векторів атак, порушень політик безпеки та нетипових моделей використання, які можуть вказувати на наявність загрози [8].

Зі свого боку, SOAR-системи функціонують як стратегічні інструменти для автоматизації реагування на виявлені інциденти. Вони стандартизують процедури реагування, забезпечують централізовану координацію між різними засобами захисту та суттєво знижують середній час реагування (Mean Time to Respond, MTTR). Інтеграція цих компонентів в єдиний контур безпеки мінімізує залежність від людського фактора – критичний аспект у високодинамічному мультихмарному середовищі – та забезпечує відповідність міжнародним стандартам безпеки, таким як NIST SP 800-53, ISO/IEC 27001 та SOC 2 [10].

Отже, синергія між засобами виявлення загроз і платформами SOAR формує основу сучасної стратегії хмарної безпеки, яка здатна не лише швидко виявляти та нейтралізовувати загрози, а й підвищувати стійкість інфраструктури до складних багатовекторних атак [7].

4. Системи виявлення загроз як основа проактивної хмарної безпеки

Функціональні можливості систем виявлення загроз значно перевищують просте виявлення вторгнень або порушень. Ці системи здійснюють глибоку інспекцію поведінки користувачів, сервісів і мережевих з'єднань шляхом застосування аналітики, що базується на політиках безпеки, сигнатурних методах, евристичних підходах та поведінкових моделях. Такий підхід дає змогу не лише виявляти очевидні інциденти, а й проактивно ідентифікувати латентні загрози, які ще не проявилися

як активні атаки, зокрема латеральний рух, спроби підвищення привілеїв або зловживання легітимними інструментами для несанкціонованих дій (так звані техніки Living off the Land, або LotL) [7].

Ключовою перевагою таких систем є їх здатність класифікувати виявлені інциденти за рівнем критичності, що дає змогу оптимізувати розподіл ресурсів безпеки та пріоритизувати дії з реагування. Це особливо важливо в умовах обмежених людських ресурсів у центрах обробки інцидентів безпеки (Security Operations Centers, SOCs) та високого рівня інформаційного шуму у вигляді хибнопозитивних спрацювань. Системи виявлення загроз можуть бути як фільтраційний шар, що не лише пригнічує незначущі події, а й збагачує дані про інциденти контекстною інформацією – такою як ідентичність користувача, уражений ресурс, географічне розташування та тип загрози [3].

У стратегічному вимірі системи виявлення загроз також виконують роль механізму зворотного зв'язку для вдосконалення політик безпеки, формування аналітичних потоків про загрози (threat intelligence feeds) та адаптації оборонних стратегій до змін у ландшафті загроз. Без цієї функціональності рішення класу SOAR не можуть працювати ефективно, оскільки структурований і якісний вихід із систем виявлення загроз слугує первинним тригером для ініціації автоматизованих сценаріїв реагування (playbooks) [8].

5. Роль систем SOAR у стратегії управління інцидентами інформаційної безпеки

Системи SOAR (Security Orchestration, Automation, and Response) становлять ключовий елемент сучасної кібербезпеки, забезпечуючи автоматизацію, координацію та стандартизацію процесів виявлення загроз, їхнього аналізу та реагування на інциденти. Їх впровадження суттєво зменшує середній час виявлення (MTTD) і середній час реагування (MTTR), знижує навантаження на аналітиків центрів моніторингу безпеки (SOC) і мінімізує ризики, пов'язані з людським фактором.

Актуальність використання SOAR особливо зростає в умовах мультихмарних середовищ, де обсяг подій безпеки, що потребують обробки, часто перевищує можливості традиційних команд реагування [6]. Системи SOAR можуть інтегруватися з широким спектром компонентів хмарної безпеки, зокрема з API платформ (AWS, Azure, GCP), системами SIEM (наприклад, Splunk), інструментами керування вразливостями, сервісами управління ідентичністю та доступом (наприклад, HashiCorp Vault), а також з інструментами обслуговування звернень [15].

Ключові функціональні можливості систем SOAR охоплюють:

- автоматизоване виявлення аномальних подій на основі даних моніторингових систем (наприклад, Prisma Cloud, GuardDuty, Splunk);
- виконання стандартизованих сценаріїв реагування (playbooks), які передбачають блокування облікових записів, ізоляцію віртуальних машин, зміну правил файрвола та генерацію повідомлень у SIEM-платформах;
- оркестрацію робочих процесів між інфраструктурними компонентами – від CMDB і EDR до платформ керування інцидентами, таких як Jira і ServiceNow;
- створення аудитованих журналів дій відповідно до стандартів NIST SP 800-61, ISO/IEC 27035, SOC 2, HIPAA тощо.

Типовий сценарій використання SOAR передбачає автоматизоване реагування на створення хмарних об'єктів у нетипових регіонах, несанкціонований доступ до API або використання привілейованих облікових записів поза робочим часом. У таких випадках система ініціює відповідні дії – відкликання ключів доступу, ізоляцію активів і сповіщення відповідальних команд.

Важливим аспектом інтеграції SOAR є його взаємодія із системами управління секретами, такими як HashiCorp Vault, що дають змогу реалізовувати Just-In-Time-доступ і усувають потребу в постійних облікових даних [22].

Отже, системи SOAR забезпечують як технічне, так і організаційне підґрунтя для побудови масштабованої, відповідної стандартам та адаптивної стратегії безпеки у хмарних середовищах. Їх впровадження суттєво скорочує час перебування зловмисника в системі, підвищує прозорість реагування та зміцнює загальну кіберстійкість організації.

5.1. Технологічна реалізація автоматизованого реагування на основі SOAR

Технологічна реалізація рішень SOAR (Security Orchestration, Automation, and Response) передбачає створення інтегрованої інфраструктури управління інцидентами інформаційної безпеки, що забезпечує автоматизацію критичних етапів – від виявлення аномалій до нейтралізації загроз. У публічних і мультихмарних середовищах, де значно зростає обсяг подій і джерел даних, SOAR стає фундаментальним елементом для забезпечення масштабованості, послідовності дій і відповідності регуляторним вимогам [15].

Архітектурно платформа SOAR виконує функцію вузла оркестрації, що взаємодіє з такими класами компонентів:

- Джерела телеметрії та подій: SIEM-системи (наприклад, Splunk, Chronicle), сервіси моніторингу та захисту хмари (Prisma Cloud, AWS GuardDuty), системи керування вразливостями, сервіси автентифікації та ідентичності (Azure AD, Okta).
- Оркестратор реагування: SOAR-рушій, який здійснює кореляцію подій, ухвалює рішення та активує сценарії реагування (playbooks) – зазвичай реалізований як окреме програмне рішення (Cortex XSOAR, Splunk SOAR).
- Шлюзи інтеграції: засоби для виконання автоматизованих дій у хмарних середовищах (AWS IAM, Azure Resource Manager), інтеграції з сервісами керування інцидентами (ServiceNow, Jira), системами управління секретами (HashiCorp Vault), інструментами автоматизації DevOps (Ansible, Terraform).

Типовий сценарій автоматизованого реагування має такий вигляд:

1. Prisma Cloud виявляє потенційно аномальну активність (наприклад, доступ до контейнера з нетипового регіону), що класифікується як подія з високим ризиком.
2. Подія передається до платформи SIEM (наприклад, Splunk), де за допомогою попередньо визначених правил кореляції формується сповіщення.
3. Платформа SOAR отримує сповіщення із SIEM і активує відповідний сценарій реагування.
4. Сценарій виконує послідовність дій:

– тимчасово призупиняє облікові дані через інтеграцію з Vault;
– ізолює підозрілий віртуальний екземпляр;
– створює інцидент у ServiceNow або Jira з відповідними атрибутами події;
– автоматично сповіщає відповідального аналітика або команду реагування.

Ключовою перевагою сучасних SOAR-рішень є можливість розробки індивідуальних сценаріїв реагування у вигляді машинно-читаних структур (YAML, JSON) із повним журналюванням відповідно до принципів audit trail. Це забезпечує прозорість і простежуваність, необхідні для відповідності таким стандартам, як ISO/IEC 27035, NIST SP 800-61, SOC 2 і PCI DSS [17].

Інтеграція SOAR із системами управління секретами (наприклад, HashiCorp Vault) дає змогу реалізовувати моделі динамічного контролю доступу, зокрема Just-In-Time Access, коли критичні привілеї надаються лише в момент виконання операцій. Це значно знижує ризик експлуатації вразливостей, пов’язаних із постійним зберіганням облікових даних [22].

Отож впровадження SOAR у хмарну інфраструктуру формує технічну й організаційну основу проактивної безпеки, мінімізує середній час реагування на інциденти (MTTR) і оптимізує координацію між підсистемами в архітектурі кібербезпеки [27].

5.2. Типові проблеми безпеки хмарної інфраструктури та роль SOAR у їх подоланні

У процесі побудови багаторівневих хмарних архітектур організації стикаються з низкою системних вразливостей, які знижують загальний рівень безпеки. До таких проблем належать фрагментовані механізми контролю доступу, відсутність централізованого нагляду за взаємодією між хмарами, людський фактор у процесах реагування, а також нестача формалізованих процедур обробки інцидентів. Ці виклики є критичними для сучасного мультихмарного середовища та потребують технологічних рішень, здатних забезпечити масштабоване, стандартизоване й автоматизоване

реагування на загрози. У цьому контексті системи SOAR (Security Orchestration, Automation, and Response) відіграють ключову роль, забезпечуючи ефективну оркестрацію процесів виявлення, аналізу й реагування на інциденти.

Нижче наведено огляд найпоширеніших проблем безпеки в хмарній інфраструктурі та механізмів їх подолання за допомогою SOAR-рішень:

1. Фрагментований доступ у мультихмарному середовищі

У разі одночасного використання кількох хмарних провайдерів (AWS, Azure, GCP) ускладнюється керування правами доступу та аудит дій користувачів. SOAR забезпечує централізовану агрегацію логів доступу й подій, що дає змогу виявляти аномальні переміщення між середовищами (lateral movement) та реалізовувати динамічні політики Zero Trust [14].

2. Відсутність стандартизованих процедур реагування

Ручне реагування, що залежить від суб'єктивного сприйняття аналітиків SOC, часто призводить до затримок або помилкових рішень. SOAR використовує заздалегідь визначені сценарії реагування (playbooks), які автоматизують розв'язання типових ситуацій, наприклад, ізоляцію ресурсів, відкликання ключів доступу або створення інцидентів у сервісних системах.

3. Людський фактор і обмежені ресурси SOC

Значна частина інцидентів не ескалується своєчасно через перевантаження аналітиків першої лінії або нестачу кваліфікації. SOAR дає змогу делегувати рутинні завдання автоматизованим механізмам – створення та оновлення записів у CMDB, обробка подій SIEM або взаємодія з Vault для обмеження прав доступу [8].

4. Відсутність прозорості та можливості аудиту дій реагування

У багатьох випадках організаціям не вдається забезпечити повний журнал дій у процесі реагування, що унеможливлює проходження сертифікацій на відповідність (SOC 2, ISO/IEC 27001, PCI DSS). SOAR формалізує й реєструє кожен крок у межах сценарію реагування із зазначенням часу, ініціатора та наслідків кожної дії.

5. Високий dwell time зловмисників

Через відсутність автоматизованого аналізу аномалій загрози можуть залишатися непоміченими протягом кількох тижнів. SOAR у поєднанні з модулями UEBA або системами SIEM (наприклад, Splunk, Sentinel) здатен ініціювати виявлення на основі поведінкових шаблонів, оперативно ескалувати інциденти та запускати заходи з локалізації загроз [26].

Отож типові проблеми безпеки в хмарному середовищі можуть бути ефективно усунуті шляхом впровадження SOAR як системного компонента. Його здатність інтегруватися з API хмарних платформ, керувати доступом через Vault, автоматизувати сценарії реагування та зберігати повний журнал подій робить його незамінним інструментом для досягнення як технологічної, так і нормативної зрілості у сфері кібербезпеки [22].

6. Порівняння SOAR-систем та обґрунтування вибору

У межах проведеного дослідження було здійснено порівняльний аналіз найпоширеніших платформ класу SOAR: Palo Alto Cortex XSOAR, Splunk SOAR, IBM QRadar SOAR та Microsoft Sentinel. Основними критеріями оцінювання були: рівень інтеграції з хмарними сервісами (AWS, Azure, GCP), гнучкість та керованість сценаріїв автоматизації (playbooks), можливості роботи з джерелами threat intelligence, масштабованість рішень у розподілених інфраструктурах, а також відповідність міжнародним стандартам інформаційної безпеки.

Результати аналізу засвідчили, що Cortex XSOAR вирізняється розвиненими можливостями створення сценаріїв автоматизації та тісною інтеграцією з платформою Prisma Cloud. Splunk SOAR характеризується високим рівнем сумісності із SIEM-рішенням Splunk та забезпечує ефективну централізацію процесів реагування. IBM QRadar SOAR має обмежену підтримку мультихмарних середовищ, що знижує його практичну придатність у гетерогенних архітектурах. Microsoft Sentinel продемонстрував високу ефективність у межах екосистеми Azure, однак його застосування у мультихмарних сценаріях є обмеженим.

Зважаючи на результати порівняння, оптимальною для реалізації поставлених у дослідженні завдань визнано комбінацію таких компонентів: Prisma Cloud (виявлення аномалій і класифікація інцидентів), Splunk SOAR (централізована автоматизація реагування), HashiCorp Vault (керування секретами) та Jenkins (засоби автоматизації змін у середовищі). Така інтегрована конфігурація забезпечує відповідність галузевим стандартам, скорочує середній час виявлення та реагування на інциденти, мінімізує вплив людського фактора та формує єдину систему превентивного захисту, моніторингу й автоматизованого усунення загроз.

7. Стандарти безпеки як основа автоматизації реагування на інциденти

Автоматизоване виявлення та реагування на інциденти в мультихмарних середовищах має ґрунтуватися на положеннях міжнародних стандартів інформаційної безпеки, серед яких ISO/IEC 27001, ISO/IEC 27035, NIST SP 800-53, SOC 2, PCI DSS та HIPAA. Зазначені нормативні документи визначають ключові вимоги щодо класифікації інцидентів, встановлення часових меж реагування, ведення журналів подій і забезпечення прозорості для аудиту. У практичній реалізації ці положення безпосередньо відображаються у платформі SOAR через автоматизоване створення інцидентів на основі сигналів SIEM, запуск стандартизованих сценаріїв реагування (playbooks), фіксацію дій у журналах та формування звітності для контролю й оцінки ефективності заходів. Отож міжнародні стандарти є методологічним підґрунтям, а SOAR – технічним інструментом їх реалізації, що забезпечує відповідність нормативним вимогам, підвищує структурованість процесів реагування та зміцнює загальну кіберстійкість хмарної інфраструктури [28].

8. Реалізація автоматизованої моделі в мультихмарному середовищі

У запропонованій архітектурі автоматизованого реагування на інциденти інформаційної безпеки центральну роль відіграє інтеграція платформи Palo Alto Prisma в публічну хмарну інфраструктуру. В умовах мультихмарного розгортання, зокрема у середовищах Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP), процеси моніторингу, виявлення загроз та реагування ускладнюються через відмінності в механізмах доступу, стандартах автентифікації та засобах ізоляції мереж. Традиційні методи, що ґрунтуються на ручному втручанні, виявляються неефективними за таких умов, оскільки не здатні забезпечити своєчасне реагування та є схильними до затримок, що збільшує ризик компрометації активів [23].

Запровадження автоматизованих підходів на базі Jenkins дає змогу побудувати логіку реагування, яка оркеструє дії безпеки згідно з наперед визначеними сценаріями. Це досягається шляхом використання автоматизованих сценаріїв (playbooks), збагачення загрозової аналітики аналітичними модулями та безперервного моніторингу інцидентів у режимі реального часу. Такі механізми дають змогу ізолювати ресурси інфраструктури ще до залучення персоналу SecOps, що суттєво скорочує час присутності зловмисника (dwell time) та знижує ризик латерального руху й ескалації [15].

Оркестрація за допомогою Jenkins реалізується через готові конектори та API, що забезпечують уніфіковану взаємодію між різними провайдерами хмарних сервісів. Це сприяє впровадженню єдиних стандартів реагування у гетерогенних хмарах без потреби створення окремих ручних процедур для кожної платформи. Ключовою перевагою є забезпечення взаємодії між інструментами безпеки, які діють як скоординована система. Це спрощує управління інцидентами, уніфікує джерела подій, дії реагування та звітність у межах централізованої платформи [20].

Застосування експертизи Palo Alto та аналітичних можливостей Prisma дає змогу виявляти нові вектори атак на основі аномальної поведінки й негайно застосовувати відповідні політики безпеки. Отримані дані далі передаються до центрів обробки інцидентів (SOC) для аналізу, що забезпечує не лише своєчасне реагування, а й накопичення знань для подальшого вдосконалення механізмів реагування.

Отже, реалізація автоматизованої моделі в мультихмарному середовищі із використанням Prisma, Jenkins та SOAR забезпечує масштабоване, ефективне та стандартизоване реагування на інциденти відповідно до вимог сучасних динамічних інфраструктур [14].

9. Сценарій автоматизованого реагування на інцидент

Запропонована архітектура автоматизації безпеки у публічних хмарних середовищах передбачає використання інтегрованих рішень для виявлення загроз, їх аналізу та виконання автоматизованих дій реагування. Цей процес реалізується шляхом поетапного виконання дій, спрямованих на ізоляцію загроз з мінімальним залученням людського ресурсу.

На початковому етапі аномалії у поведінці хмарної інфраструктури виявляються за допомогою Prisma Cloud (рис. 1) (Крок 1). Ці аномалії, які можуть свідчити про потенційні інциденти безпеки, передаються до Splunk для подальшої обробки (Крок 2). У середовищі Splunk дані аналізуються з метою визначення критичності подій, після чого формується список “значущих подій” (notable events), що потребують реагування.

Рішення щодо подальших дій приймає команда SecOps рівня 2 (L2) (Крок 3), яка отримує сповіщення про критичні події через Splunk (Крок 4). Команда SecOps очікує відповіді від кінцевого користувача протягом 15 хвилин, після чого – у разі її відсутності – запускається процедура блокування за допомогою автоматизованих механізмів. У разі підтвердження загрози команда активує автоматизовану дію SOAR під назвою “RedButton” (Крок 5). Ця дія викликає автоматизаційний скрипт у Splunk SOAR, який ініціює виконання задачі на вузлі Jenkins (Крок 6).

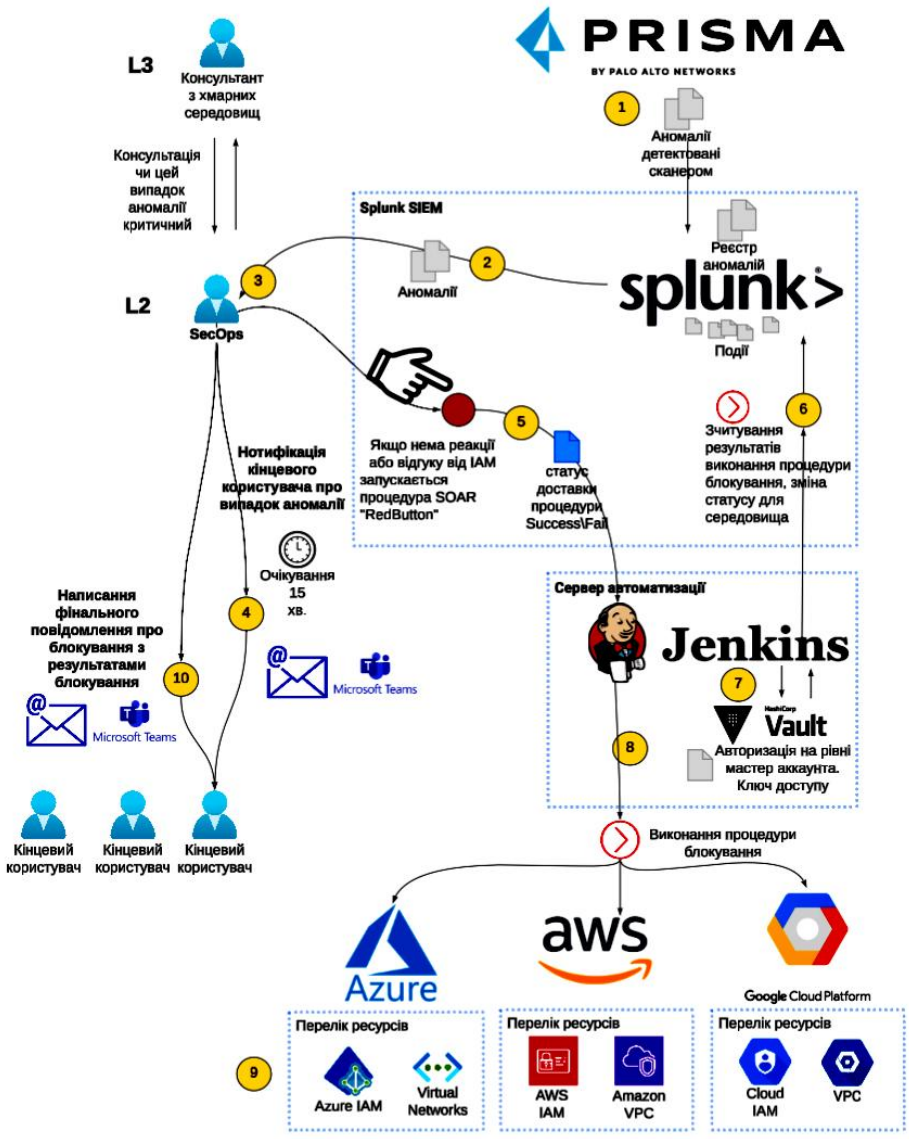

Рис. 1. Процес автоматизованого реагування на інцидент інформаційної безпеки

Jenkins виконує функції координаційного вузла, отримуючи необхідні облікові дані для доступу до платформ публічних хмар (AWS, Azure, Google Cloud Platform) із системи управління секретами HashiCorp Vault (Крок 7). Це забезпечує безпечне використання облікових даних для виконання блокувальних дій у хмарній інфраструктурі.

Далі Jenkins застосовує відповідні політики ізоляції, визначені у попередньо сконфігурованих плейбуках (Крок 8). У Google Cloud Platform це може включати блокування доступу через Cloud IAM або зміну параметрів віртуальної мережі (VPC). У середовищі AWS здійснюється деактивація скомпрометованих облікових записів IAM, зміна правил груп безпеки або обмеження доступу через VPC. У Microsoft Azure ізоляція реалізується шляхом модифікації правил Azure IAM або обмеження мережевих під'єднань через віртуальні мережі. Важливо підкреслити, що ізольовані ресурси залишаються функціональними, що дає змогу уникнути повної зупинки інфраструктурних операцій (Крок 9) .

Після виконання відповідних дій кінцеві користувачі та адміністратори отримують сповіщення про інцидент за допомогою електронної пошти або Microsoft Teams. Повідомлення містять детальну інформацію щодо характеру загрози, вжитих заходів та подальших рекомендацій.

Фінальним етапом є формування звіту типу post-mortem, який містить аналіз причин виникнення інциденту, його наслідків, виконаних дій і рекомендацій щодо запобігання подібним ситуаціям у майбутньому. Такий звіт має на меті вдосконалення процесів реагування та підвищення загальної ефективності системи інформаційної безпеки (Крок 10).

Результати дослідження

З метою оцінювання ефективності запропонованої моделі було проведено експериментальне тестування у контрольованому середовищі, що відтворює мультихмарну інфраструктуру підприємства. Основними показниками аналізу визначено середній час виявлення інциденту (Mean Time to Detect, MTTD), середній час реагування (Mean Time to Respond, MTTR) та рівень хибнопозитивних інцидентів. Отримані результати (табл. 2) продемонстрували істотне зниження значень MTTD та MTTR, а також помітне скорочення кількості хибнопозитивних спрацювань. Це свідчить про підвищення загальної ефективності моделі та підтверджує доцільність застосування автоматизованого реагування на інциденти у мультихмарних середовищах.

Таблиця 2

Результати порівняльного аналізу

Показник	Без автоматизації (оцінка на 2025 рік)	З автоматизованим реагуванням	Покращення (%)
Середній час виявлення (MTTD), годин	2,5	0,15	93
Середній час реагування (MTTR), годин	5,5	1	81
Частка хибнопозитивних інцидентів (%)	14	5	64
Навантаження на аналітиків SOC (%)	100	40	60
Прямі втрати на інцидент (USD)	1700	320	81
Потенційний вплив (оцінка ризику, з 10 балів)	8	2	75

1. Результати впровадження та напрями подальшого розвитку

Запропонована модель автоматизованого управління інцидентами в публічному хмарному середовищі була реалізована шляхом інтеграції сучасних інструментів виявлення, аналізу та реагування. Основні компоненти містять Prisma Cloud від Palo Alto Networks як основну платформу для виявлення ризиків, Splunk SOAR як систему оркестрації та автоматизації реагування, Jenkins як механізм виконання змін на рівні інфраструктури та HashiCorp Vault для безпечного управління обліковими даними. Усі елементи взаємопов'язані в межах замкненого циклу автоматизованого

реагування (виявити → проаналізувати → відреагувати → задокументувати), що функціонує в режимі реального часу без участі оператора.

Модель адаптована до мультихмарної інфраструктури, яка охоплює понад 400 хмарних облікових записів у середовищах AWS, Azure та GCP, з урахуванням типових особливостей, таких як розподіл активів, динамічне масштабування та гетерогенність механізмів автентифікації й політик контролю доступу. Архітектура відповідає принципам Zero Trust, забезпечуючи ізоляцію середовищ, перевірку кожного запиту на доступ у режимі реального часу та динамічне управління привілеями.

З практичного погляду система дає змогу своєчасно реагувати на інциденти, зокрема:

- компрометацію облікових даних через витік секретів або несанкціонований доступ;
- виявлення географічних або поведінкових аномалій сесій;
- несанкціоновану модифікацію інфраструктури або порушення політик;
- виконання підозрілих API-запитів або спроби підвищення привілеїв.

У разі виникнення інциденту система автоматично виявляє ризик за допомогою Prisma Cloud, генерує подію в Splunk, яка надалі трансформується за допомогою сценарію реагування (playbook) у дію на рівні інфраструктури (наприклад, блокування VPC або IAM), ініціює безпечне отримання тимчасових облікових даних через Vault і виконує дію за допомогою Jenkins. Усі етапи фіксуються в журналах, а після завершення формується звіт про інцидент [18].

2. Результати впровадження

Практична цінність цієї моделі полягає у її здатності забезпечити централізоване управління інцидентами в середовищі з більш ніж 400 хмарними обліковими записами. Згідно з аналітичним звітом IBM Cost of a Data Breach Report 2023, середня вартість витоку даних у хмарі становить 4,45 мільйона доларів США [22], а час перебування зловмисника в системі без виявлення (dwell time) може перевищувати 20–30 днів. Запроваджена модель знижує dwell time до кількох годин, скорочує середній час виявлення (Mean Time to Detect, MTTD) до хвилин і зменшує середній час реагування (Mean Time to Respond, MTTR) до годин, що в сукупності дає змогу знизити фінансові ризики більш ніж на 80 % порівняно з ручною обробкою інцидентів [17].

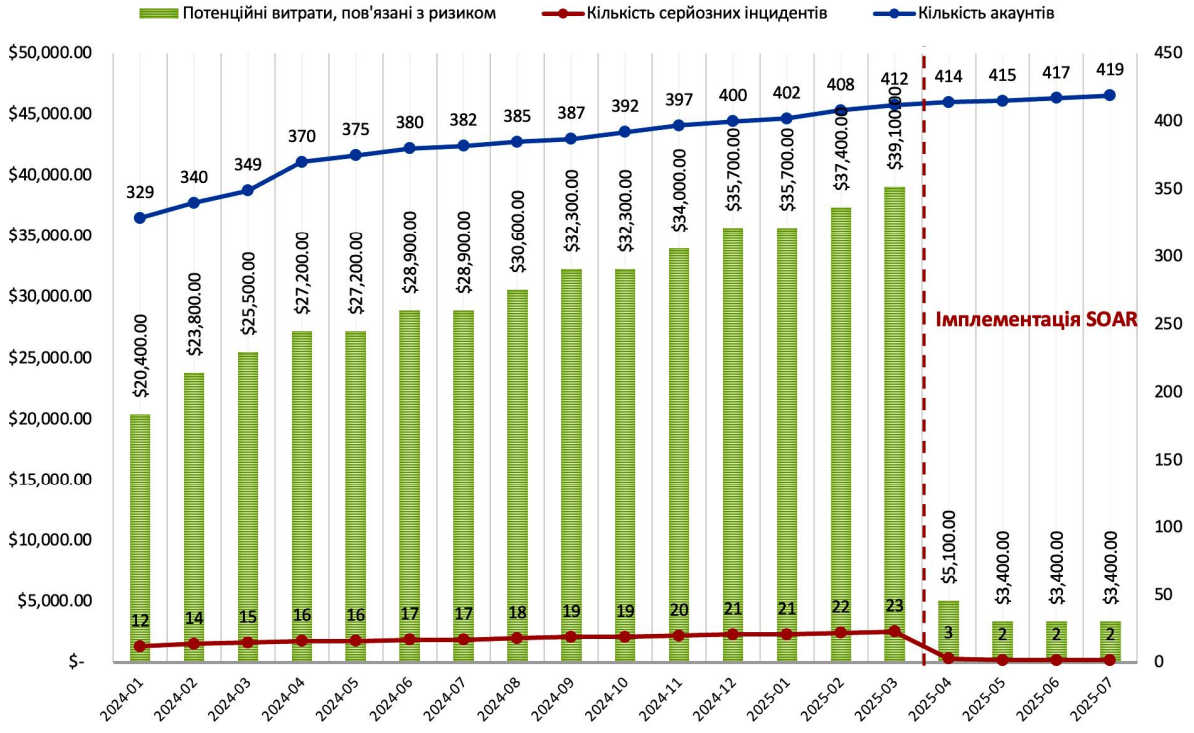

Рис. 2. Зниження вартості ризиків після впровадження SOAR

Запропоноване рішення було впроваджене в складному мультихмарному середовищі, яке охоплює три основні платформи публічних хмар – Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP), – із загальною кількістю активних облікових записів, що досягла 419 станом на середину 2025 року. Це середовище було спеціально обране з метою відтворення масштабів і операційної різноманітності реальних корпоративних інфраструктур, забезпечуючи репрезентативну основу для 19-місячного емпіричного оцінювання ефективності, адаптивності та масштабованості моделі автоматизованого реагування на інциденти, побудованої за принципами SOAR.

До впровадження рішення у березні 2025 року центр реагування на інциденти (SOC) здебільшого покладався на ручну обробку інцидентів. У цей період середньомісячний рівень ризику, пов'язаного з хмарною інфраструктурою, коливався в межах від 20 000 до 39 000 дол. США. Основними причинами цього були постійні несанкціоновані спроби доступу, витоки конфіденційних секретів, неправильні конфігурації хмарних сервісів і відсутність механізмів виявлення загроз у реальному часі. Відсутність стандартизації, автоматизації та міжхмарної видимості не лише уповільнювала процес реагування, а й створювала значне когнітивне навантаження на аналітиків першої лінії. Як наслідок, річний потенційний фінансовий вплив оцінювався у понад 370 000 дол. США.

З метою усунення зазначених операційних недоліків у березні 2025 року було впроваджено інтегровану модель реагування на інциденти, яка використовує Prisma Cloud для виявлення загроз і Splunk SOAR для оркестрації та автоматизації. Архітектура рішення забезпечила надходження телеметрії з різнорідних хмарних середовищ у реальному часі, її кореляцію, виконання автоматизованих сценаріїв реагування на критичні типи інцидентів, перевірку дій користувачів на відповідність політикам безпеки, а також обробку стандартних ситуацій без залучення ескалацій. Перехід від реактивного до напівавтономного підходу до реагування значно прискорив прийняття рішень і знизив кількість хибнопозитивних спрацювань.

Упродовж лише чотирьох місяців після впровадження кількість серйозних інцидентів різко скоротилася до 2–3 на місяць, а фінансові ризики зменшилися до діапазону 3 400–5 100 дол. США щомісячно (рис. 2). Таке суттєве зниження як операційного навантаження, так і фінансових ризиків чітко демонструє практичну ефективність рішення в протидії частим та впливовим загрозам.

Враховуючи історичну динаміку витрат, загальний обсяг економії, досягнутий протягом цієї початкової фази після впровадження, перевищив 130 000 дол. США, незважаючи на порівняно короткий період спостереження. Отримані результати підтверджують економічну доцільність та стратегічну цінність інтеграції механізмів автоматизованого реагування в масштабовані, динамічні хмарні середовища, особливо в організаціях, які стикаються зі зростаючими вимогами до відповідності, видимості та операційної стійкості.

3. Напрями подальшого розвитку

Подальший розвиток моделі передбачається за такими стратегічними напрямами:

1. Інтеграція аналітики на основі AI/ML. Використання алгоритмів машинного навчання дасть змогу покращити пріоритизацію інцидентів, зменшити кількість хибнопозитивних спрацьовувань і забезпечити динамічну адаптацію стратегій реагування на основі поведінкових шаблонів, часу доби та рівня доступу.

2. UEBA (User and Entity Behavior Analytics). Впровадження поведінкового аналізу користувачів і сервісів дасть змогу виявляти приховані атаки, латеральний рух, використання неактивних облікових записів і неочевидні аномалії, які залишаються непоміченими у традиційних сигнатурних системах.

3. Поглиблення моделі Zero Trust. Система буде розширена завдяки впровадженню динамічного контролю доступу, умовної авторизації, мікросегментації хмарної інфраструктури та жорсткого контролю міжрегіонального трафіку.

4. Автоматизація постінцидентного аналізу та самонавчання. Буде реалізовано механізми автоматизованого постінцидентного аналізу, які дозволять не лише фіксувати події, а й будувати

причинно-наслідкові графи, формулювати рекомендації щодо вдосконалення політик безпеки та динамічно оновлювати сценарії реагування (playbooks).

5. Аудит і контроль на основі метрик. Розробка розширених звітів і дашбордів для моніторингу ключових метрик безпеки (MTTD, MTTR, dwell time, рівень alert fatigue, показники покриття вимог) дасть змогу організаціям прозоро оцінювати ефективність системи, забезпечити відповідність стандартам (SOC 2, ISO/IEC 27001, NIST 800-53) і готуватись до зовнішніх аудитів.

6. Розширення адаптивності сценаріїв реагування. Завдяки використанню механізмів розгалуження й контекстного реагування в Splunk SOAR можливо реалізувати динамічні сценарії реагування, які автоматично враховують тип ресурсу, контекст події, чутливість даних і критичність бізнес-процесів.

Запропонована модель не лише відповідає сучасним вимогам щодо гнучкості реагування, автоматизації процесів і відповідності регуляторним нормам, а й закладає основу для побудови самонавчальної, інтелектуальної архітектури хмарної безпеки, орієнтованої на принципи Data-Driven Security та Continuous Adaptive Risk and Trust Assessment (CARTA).

Висновки

У межах проведеного дослідження було розроблено архітектурну модель автоматизованого управління інцидентами інформаційної безпеки в публічних хмарних середовищах, засновану на інтеграції Prisma Cloud, Splunk SOAR, Jenkins та HashiCorp Vault. Запропонована модель забезпечує наскрізну автоматизацію циклу реагування на інциденти – від виявлення аномалій до виконання коригувальних дій в інфраструктурі – без участі оператора. Такий підхід суттєво скорочує час реагування (MTTR), мінімізує вплив людського фактора та знижує ризики, пов’язані з тривалим перебуванням зловмисника в середовищі.

Аналіз реальних випадків компрометації хмарних середовищ виявив ключові вразливості, зокрема відсутність ефективного моніторингу, слабкі механізми автентифікації, брак кореляції подій та нездатність оперативно реагувати на інциденти. Запропоноване рішення усуває ці недоліки завдяки гнучкій логіці сценаріїв (playbooks), інтеграції з джерелами загрозової аналітики та контролю активності в межах моделі Zero Trust.

Наукова новизна дослідження полягає в синтезі принципів SOAR, Zero Trust, ML-аналітики та UEBA в єдину архітектуру, адаптовану до мультихмарної інфраструктури, що охоплює понад 400 хмарних облікових записів. Розроблена модель не лише автоматизує реагування на інциденти, а й забезпечує масштабоване впровадження політик безпеки без втрати контролю, що є критично важливим для сучасних підприємств, які управляють великою кількістю хмарних ресурсів.

З практичного погляду впровадження описаного рішення дає змогу організаціям знизити ризик фінансових втрат, пов’язаних із компрометацією хмарного середовища. Відповідно до застосованої моделі оцінювання ризиків відсутність автоматизованого управління інцидентами може призвести до щорічних втрат у сотні тисяч доларів через затримки в реагуванні, витоки даних та простої систем.

Подальші напрями дослідження передбачають удосконалення механізмів поведінкового аналізу інцидентів із використанням методів машинного навчання, розширення підтримки платформ завдяки динамічній API-інтеграції, а також впровадження механізмів самонавчання на основі історичних сценаріїв реагування. Додатково рекомендовано формалізувати підхід до відповідності нормативним вимогам (NIST, ISO, SOC 2) через автоматизований аудит і контроль виконання політик.

Список літератури

1. Vakhula O., Opirskyy I., Mykhaylova O. Research on Security Challenges in Cloud Environments and Solutions based on the “security-as-Code” Approach (2023). CEUR Workshop Proceedings, 3550, pp. 55–69.

2. Vasylyshyn S., Susukailo V., Opirskyy I., Kurii Y., Tyshyk I. A model of decoy system based on dynamic attributes for cybercrime investigation, Eastern-European J. Enterp. Technol. 1.9 (121) (2023) 6–20. DOI: 10.15587/1729-4061.2023.273363.

3. Suram, Kiran. (2025). Innovations in Infrastructure Automation: Advancing IAM in Cloud Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 11. 255–263. DOI: 10.32628/CSEIT25111223.

4. Soldatenko, D. & Vik,. (2022). Study of efficiency of using it-infrastructure-as-a-service for cloud computing. System technologies. 2. 68–76. DOI: 10.34185/1562-9945-2-139-2022-07.

5. Narayanasamy, Deneesh. (2025). Transforming Healthcare with Secure Cloud Infrastructure. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 11. 633–644. DOI: 10.32628/CSEIT25111271.

6. Thokala, Vasudhar Sai. (2023). Scalable Cloud Deployment and Automation for E-Commerce Platforms Using AWS, Heroku, and Ruby on Rails. International Journal of Advanced Research in Science, Communication and Technology. 349–362. DOI: 10.48175/IJARSCT-13555A.

7. Narayanan, Pavan. (2024). Engineering Data Pipelines Using Google Cloud Platform. DOI: 10.1007/979-8-8688-0602-5_16.

8. Sreerangapuri, Ashok. (2024). Blockchain-Enabled AI Governance for Scalable Cloud Security Automation. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY. 15. 947–959. DOI: 10.5281/zenodo.13962366.

9. Ramya J. (2024). Data-Driven Framework for Cloud Storage Security Optimization: Leveraging Predictive Analytics and Machine Learning to Enhance Threat Detection and Incident Response. Journal of Electrical Systems. 20. 6646–6653. DOI: 10.52783/jes.6721.

10. Torkura, Kennedy & Sukmana, Muhammad Ihsan Haikal & Cheng, Feng & Meinel, Christoph. (2020). Continuous Auditing & Threat Detection in Multi-Cloud Infrastructure. DOI: 10.36227/techrxiv.13108313.

11. Christian, Juan & Paulino, Luis & Sá, Alan. (2022). A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response. DOI: 10.1007/978-3-031-21280-2_7.

12. Rehan, Hassan. (2022). Zero-Trust Architecture for Securing Multi-Cloud Environments. 2. 236–273.

13. Abbas, Munawar & Iqbal, Javid. (2025). Autonomous Threat Response Systems: A New Paradigm for Intelligent Cloud Security Automation. DOI: 10.13140/RG.2.2.13750.20800.

14. Pitkar, Harshad. (2025). Cloud Security Automation Through Symmetry: Threat Detection and Response. Symmetry. 17. 859. DOI: 10.3390/sym17060859.

15. Mahida, Ankur. (2023). Real-Time Incident Response and Remediation-A Review Paper. Journal of Artificial Intelligence & Cloud Computing. 1–3. DOI: 10.47363/JAICC/2023(2)247.

16. Martseniuk, Y., Partyka, A., Harasymchuk, O., Cherevyk V. and Dovzhenko N. Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management (2025) CEUR Workshop Proceedings, 3991, pp. 260–274.

17. Varadaraj, Prabhu. (2025). Multi-Cloud and Hybrid Infrastructure: Addressing Consistency Challenges Across Cloud Providers. International Journal of Advanced Research in Science, Communication and Technology. 520–526. DOI: 10.48175/IJARSCT-24465.

18. Smith, John & Johnson, Emily & Patel, Raj & Christopher, George. (2023). Enhancing Cloud Security Incident Response with AI and Big Data Integration.

19. Mercy, Olaosegba. (2023). Holistic Security Solutions for Complex Multi- Cloud Ecosystems. International Journal of Novel Research and Development.

20. Jangampet, Vinay & Pulyala, Srinivas & Desetty, Avinash. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 10. 1545–1549. DOI: 10.61841/turcomat.v10i3.14323.

21. Ismail & Kurnia, Rahmat & Brata, Zilmas & Nelistiani, Ghitha & Heo, Shinwook & Kim, Hyeongon & Kim, Howon. (2025). Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence. Information. 16. 365. DOI: 10.3390/info16050365.

22. Vast, Rahul & Sawant, Shruti & Thorbole, Aishwarya & Badgujar, Vishal. (2021). Artificial Intelligence based Security Orchestration, Automation and Response System. 1–5. DOI: 10.1109/I2CT51068.2021.9418109.

23. Aljahdali, Asia & Alsulami, Raghad. (2025). Streamlining threat response and automating critical use cases with security orchestration, automation and response (SOAR). Journal of Digital Security and Forensics. 2. DOI: 10.29121/digisecforensics.v2.i1.2025.45.

24. Lee, Minkyung & Jang-Jaccard, Julian & Kwak, Jin. (2022). Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment. Computers, Materials & Continua. 73. 199–223. DOI: 10.32604/cmc.2022.028495.

25. Gunnam, Vinodh & Kilaru, Naresh Babu & Cheemakurthi, Sai Krishna Manohar. (2023). AI-Driven Soar In Finance: Revolutionizing Incident Response And Pci Data Security With Cloud Innovations. 5. 974–980. DOI: 10.35629/5252-0502974980.

26. Dakic, Vedran & Morić, Zlatan & Kapulica, Ana & Regvart, Damir. (2024). Leveraging Microsoft sentinel and logic apps for automated cyber threat response. Edelweiss Applied Science and Technology. 8. 4319–4348. DOI: 10.55214/25768484.v8i6.2933.

27. Karlzen, Henrik & Sommestad, Teodor. (2023). Automatic incident response solutions: a review of proposed solutions' input and output. 1–9. DOI: 10.1145/3600160.3605066.

28. Gulati, Samridhi & Tyagi, Ayushi & Goel, Pawan. (2024). Security Automation and Orchestration in the Cloud. DOI: 10.4018/979-8-3693-3249-8.ch002.

AUTOMATE CLOUD SECURITY INCIDENT MANAGEMENT WITH A SOAR-BASED APPROACH

O. S. Sapsai, Y. V. Martseniuk, A. I. Partyka

Lviv Polytechnic National University,
Department of Information Protection

Modern organizations increasingly integrate public cloud platforms such as AWS, Azure, and Google Cloud Platform into their infrastructure to enhance flexibility and scalability. However, multi-cloud environments introduce new cybersecurity challenges. Human factors and careless handling of access parameters to cloud resources can create serious threats. In particular, if an attacker gains access to authorization keys, they can not only control existing resources but also create new ones for malicious purposes–such as launching attacks, distributing malware, or mining cryptocurrencies. Such incidents can rapidly cause financial losses, undermine user trust, and disrupt the stability of critical services.

This study explores the use of Splunk SOAR (Security Orchestration, Automation, and Response) as a tool for automated detection, analysis, and response to threats in public cloud environments. The primary focus is on integrating Splunk SOAR with cloud providers' APIs to dynamically block compromised resources and to implement detailed response playbooks that isolate threats at the level of individual components (virtual machines, network policies, user accounts).

The paper also analyzes the integration of Splunk anomaly detection with Palo Alto Prisma as a comprehensive deviation scanner, the use of HashiCorp Vault for credentials protection, the introduction of a quarantine mode for isolating compromised resources, and the improvement of incident response processes.

The results demonstrate that automating security processes with Splunk SOAR significantly reduces response time, minimizes the impact of the human factor, and lowers the risk of cloud infrastructure compromise. The proposed approach strengthens an organization's resilience to threats in a multi-cloud environment, ensuring an optimal balance between security, availability, and operational efficiency.

Keywords: Cloud security, public cloud environments, multi-cloud infrastructure, Splunk SOAR, automated incident response, incident management, threat mitigation, resource blocking, anomaly monitoring, cloud provider APIs, security operations, automation, DevOps, threat intelligence, human factor.