COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.160

УДК 004.056.5

ОГЛЯД ФУНДАМЕНТАЛЬНОЇ МОДЕЛІ БЕЗПЕЧНОЇ ОРКЕСТРАЦІЇ, АВТОМАТИЗАЦІЇ ТА РЕАГУВАННЯ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНИХ МЕРЕЖ

О. Ю. Котляров, Л. Л. Бортнік

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: oleksandr.y.kotliarov@lpnu.ua, leonid.l.bortnik@lpnu.ua

Проаналізовано фундаментальну модель SOAR (Security Orchestration, Automation, and Response) у контексті кібербезпеки віртуальних мереж. Охарактеризовано синтез основних концепцій оркестрації, автоматизації та реагування, які є критичними елементами сучасних підходів до управління ризиками та захисту інформаційних систем. Особлива увага приділена інтеграції SOAR із наявними технологіями кібербезпеки, такими як SIEM, EDR, XDR, що дає змогу формувати єдину екосистему безпеки, забезпечуючи швидке виявлення загроз, їх класифікацію та оперативне реагування.

Розглянуто класифікацію загроз, притаманних децентралізованим і мультихмарним середовищам, таких як атаки на рівні протоколів, злом даних і внутрішні порушення, а також акцентовано на специфічних викликах, зокрема динамічності конфігурації мереж та масштабованості безпекових рішень. Проведено порівняльний аналіз відповідності моделі SOAR міжнародним стандартам кібербезпеки (NIST, ISO 27001), який демонструє її здатність до уніфікації підходів і автоматизації процедур відповідності нормативним вимогам.

Дослідження також охоплює перспективні напрями розвитку SOAR, зокрема впровадження штучного інтелекту та самонавчальних алгоритмів для адаптивного управління загрозами, використання цифрових двійників для моделювання безпекових сценаріїв та адаптацію до викликів квантових обчислень. Окремо висвітлено роль великих даних у покращенні функцій SOAR, зокрема у зменшенні хибнопозитивних спрацювань і виявленні багатовекторних атак.

Результати цього дослідження мають прикладний характер і спрямовані на вдосконалення інструментів кібербезпеки для забезпечення комплексного захисту віртуалізованих середовищ. Зроблено висновок, що модель SOAR є ключовим компонентом у формуванні стратегічних підходів до захисту інформаційних активів в умовах еволюції кіберзагроз.

Ключові слова: кібербезпека, SOAR, автоматизація, мультихмарні середовища, управління ризиками, стандарти безпеки, віртуальні мережі, мережевий трафік.

Вступ

У контексті епохи стрімкої діджиталізації, що супроводжується експоненційним зростанням складності інформаційних систем, проблема забезпечення кібербезпеки стає одним із ключових викликів сучасності. Віртуалізація мережевих ресурсів, яка відкрила нові горизонти масштабованості та гнучкості інфраструктури, одночасно породила нові вектори атак, що значно ускладнює забезпечення їх цілісності, конфіденційності та доступності. У таких умовах традиційні методи реагування та управління безпекою демонструють суттєві обмеження через недостатню швидкість адаптації до нових загроз та обмеження у можливостях інтеграції різних рішень [1].

Одним із революційних підходів до розв'язання зазначених проблем стала концепція SOAR (Security Orchestration, Automation, and Response), яка об'єднує можливості оркестрації, автоматизації процесів та оперативного реагування на інциденти. Ця модель спрямована на синергетичну взаємодію між різноманітними інструментами кібербезпеки, їх інтеграцію в єдину екосистему та мінімізацію впливу людського фактора на процеси захисту інфраструктури. Завдяки цьому SOAR не лише підвищує ефективність реагування на загрози, а й забезпечує динамічну адаптацію системи до змінних умов кіберсередовища [2, с. 29].

Мета цього дослідження полягає в аналізі фундаментальної моделі SOAR у контексті кібербезпеки віртуальних мереж, зокрема, в оцінці її основних компонентів, практичного потенціалу та перспектив розвитку.

Дослідження є важливим у світлі постійного еволюційного зростання кількості та складності кіберзагроз, що потребує нових підходів до захисту інформаційних активів, особливо в умовах віртуальних мереж, які, з одного боку, спрощують управління ресурсами, а з іншого – стають мішенню для атак. Результати роботи сприятимуть поглибленню розуміння ролі SOAR у забезпеченні комплексної безпеки віртуалізованих середовищ та слугуватимуть базою для подальших досліджень у цій сфері.

Огляд літературних джерел

Останні дослідження у сфері кібербезпеки зосереджені на вивченні автоматизації процесів виявлення та реагування на загрози, що є основою моделі SOAR (Security Orchestration, Automation, and Response). У науковому дискурсі ця тематика активно досліджується з позицій інформаційної безпеки, управління ризиками, інтеграції зі сучасними технологіями та відповідності міжнародним стандартам.

Зокрема, праця [5] висвітлює загальні аспекти застосування SOAR у кібербезпеці віртуальних мереж, зокрема інтеграцію з такими системами, як SIEM, EDR і XDR. Дослідження [3] та [4] акцентують увагу на автоматизації робочих процесів у центрах безпеки (SOC), що значно зменшує навантаження на аналітиків та підвищує швидкість реагування.

Д. Шевчук та ін. [2] аналізують питання безпечної аутентифікації, авторизації та контролю доступу в інформаційних системах, що є важливим аспектом впровадження SOAR. У праці [7] розглянуто питання взаємодії SOAR з платформами штучного інтелекту та машинного навчання для покращення виявлення аномалій у мережевому трафіку.

Суттєве значення для розвитку SOAR має інтеграція з міжнародними стандартами кібербезпеки, що досліджено у працях [6] та [20], які аналізують відповідність SOAR вимогам NIST та ISO/IEC 27001.

Отже, сучасні дослідження вказують на перспективність розвитку SOAR як ключового компонента автоматизації безпеки, що поєднує виявлення, аналіз та реагування на інциденти в єдиній екосистемі захисту інформаційних активів.

Постановка задачі

У сучасних умовах цифровізації та зростання складності інформаційних систем забезпечення кібербезпеки стає критично важливим завданням. Віртуалізовані мережі, що пропонують гнучкість

та масштабованість, одночасно створюють нові виклики, пов’язані з розширенням поверхні атак та необхідністю швидкого реагування на загрози. Традиційні методи безпеки виявляються недостатньо ефективними через високий рівень динамічності кіберзагроз, що потребує нових підходів до управління ризиками.

Основною задачею дослідження є аналіз моделі SOAR (Security Orchestration, Automation, and Response) як інструменту підвищення ефективності кібербезпеки віртуальних мереж. Зокрема, дослідження має на меті:

1. Визначити основні компоненти SOAR та їхню роль у забезпеченні безпеки віртуалізованих середовищ.
2. Дослідити інтеграцію SOAR із сучасними кібербезпековими рішеннями, такими як SIEM, EDR, XDR, для створення єдиної екосистеми захисту.
3. Оцінити ефективність використання SOAR для автоматизації реагування на інциденти, мінімізації людського фактора та прискорення нейтралізації загроз.
4. Провести аналіз відповідності SOAR міжнародним стандартам кібербезпеки (NIST, ISO 27001) з метою уніфікації процедур безпеки.
5. Визначити перспективні напрями розвитку SOAR.

Результати дослідження сприятимуть розвитку підходів до захисту віртуалізованих середовищ та створенню стратегічних механізмів кібербезпеки в умовах постійно змінюваного цифрового ландшафту.

Практичне застосування моделі SOAR у віртуальних мережах

Застосування моделі SOAR (Security Orchestration, Automation, and Response) у віртуальних мережах відкриває нові горизонти для управління кібербезпекою, забезпечуючи інтеграцію автоматизованих процесів із розподіленими інструментами моніторингу та реагування. У сучасних мультихмарних і контейнеризованих середовищах SOAR забезпечує уніфіковане управління інцидентами через автоматизацію рутинних операцій, оркестрацію складних сценаріїв взаємодії систем безпеки та зниження часу реагування на загрози. Це дає змогу підвищити ефективність безпекових операцій, мінімізувати людський фактор і оптимізувати адаптацію до динамічних змін у конфігурації мережевої інфраструктури.

Ключові сценарії використання SOAR

Моніторинг та реагування на інциденти у реальному часі.

Модель SOAR забезпечує можливість оперативного виявлення та нейтралізації кіберзагроз шляхом автоматизації процесів моніторингу та аналізу інцидентів у реальному часі. Основні аспекти цього сценарію охоплюють:

– ввтоматизований аналіз даних: використання аналітичних модулів для обробки логів, телеметрії та інших джерел даних у реальному часі з метою ідентифікації аномальної активності;

– пріоритизацію інцидентів: інтеграція алгоритмів машинного навчання для ранжування загроз за ступенем їх критичності, що знижує перевантаження аналітиків безпеки;

– швидке реагування: автоматизоване виконання дій, таких як ізоляція компрометованих вузлів, блокування шкідливого трафіку або застосування правил фаєрвола, з мінімальним втручанням людини [12, с. 80].

Це дає змогу знизити час виявлення та нейтралізації загроз (MTTD і MTTR), підвищуючи стійкість віртуальних мереж до атак.

Інтеграція з існуючими продуктами безпеки.

SOAR є оркестраційним шаром, який доповнює вже впроваджені рішення з кібербезпеки, такі як SIEM, EDR, XDR (Extended Detection and Response) та інші інструменти.

Переваги інтеграції SOAR з іншими продуктами:

– уніфікована платформа управління: консолідація даних із різних систем безпеки дає змогу створювати єдину точку доступу для аналізу та реагування на загрози;

– автоматизація міжсистемної взаємодії: забезпечується автоматичне виконання складних сценаріїв, що містять кілька інструментів. Наприклад, після виявлення загрози SIEM може ініціювати відповідну дію в EDR через SOAR;

– покращення якості даних: завдяки агрегації та нормалізації даних зменшується кількість хибнопозитивних інцидентів, що спрощує роботу команд безпеки [13, с. 75].

SOAR не замінює існуючі інструменти, а постає як інтеграційна платформа, яка підвищує їхню ефективність.

Адаптація до мультихмарних середовищ.

Сучасні віртуальні мережі дедалі частіше побудовані на базі мультихмарних архітектур, що створює унікальні виклики для забезпечення безпеки. SOAR пропонує гнучкі рішення, які адаптуються до таких середовищ:

– автоматизація політик безпеки: SOAR дає змогу розгортати уніфіковані правила безпеки в декількох хмарних провайдерах, таких як AWS, Azure та Google Cloud, незалежно від їхніх особливостей;

– розширена видимість: завдяки інтеграції з хмарними API SOAR забезпечує централізований моніторинг усіх компонентів мультихмарної інфраструктури, включаючи контейнери, сервери та сервіси;

– сумісність із різними стандартами: у мультихмарному середовищі SOAR дає змогу враховувати специфічні вимоги кожного провайдера безпеки, забезпечуючи відповідність локальним і міжнародним стандартам, таким як GDPR або NIST.

Це робить SOAR незамінним інструментом у масштабних розподілених середовищах, де необхідно забезпечити безперебійну взаємодію між різними хмарними платформами та інструментами безпеки [14, с. 16].

Впровадження моделі SOAR у віртуальних мережах супроводжується низкою викликів, які зумовлені як технічними, так і організаційно-економічними факторами. Одним із ключових бар'єрів є технічні обмеження, що стосуються сумісності та масштабованості системи. Багато організацій стикаються з проблемою інтеграції SOAR із вже існуючими інструментами кібербезпеки, такими як SIEM, EDR або хмарні API, які мають різні архітектурні принципи та стандарти. Непередбачувана динамічність віртуальних мереж, зокрема автоматизоване створення та видалення ресурсів, ставить під сумнів можливість забезпечення належної масштабованості рішень SOAR, особливо в контексті мультихмарних середовищ.

Окремий аспект викликів стосується людського фактора. Високий рівень автоматизації, характерний для SOAR, потребує від фахівців нових навичок, зокрема, глибокого розуміння сценаріїв оркестрації, знання мов програмування для налаштування автоматизованих процедур та досвіду роботи з розподіленими архітектурами. Проте на сучасному етапі кібербезпеки спостерігається гостра нестача кадрів, здатних відповідати цим вимогам. Це створює значні ризики, пов'язані з неефективним використанням SOAR або навіть його некоректною конфігурацією, що може призвести до нових вразливостей.

Економічна складова є ще одним вагомим бар'єром для впровадження SOAR. Початкові витрати на інтеграцію цієї технології в інфраструктуру організації є значними, оскільки вони включають ліцензування програмного забезпечення, адаптацію до специфічних вимог середовища, навчання персоналу та створення політик безпеки. Крім того, підтримка SOAR у робочому стані потребує постійних фінансових вкладень у вигляді оновлень, адаптації до нових загроз і технологій та залучення зовнішніх консультантів для оптимізації процесів. У результаті це обмежує можливості використання SOAR невеликими організаціями, які мають обмежений бюджет на кібербезпеку, що знижує загальний рівень захищеності віртуальних середовищ.

Отже, хоча SOAR має значний потенціал для трансформації підходів до кібербезпеки, його впровадження потребує вирішення комплексу технічних, кадрових та економічних проблем, які суттєво впливають на ефективність цієї моделі у практичному застосуванні.

Оцінка ефективності SOAR

Визначення ключових показників ефективності (KPI) є критичним етапом для оцінки успішності впровадження моделі SOAR у віртуальних мережах. Основні KPI мають враховувати як технічні, так і операційні аспекти роботи системи. До найважливіших показників належать:

– час виявлення загроз (Mean Time to Detect, MTTD): скорочення MTTD свідчить про здатність системи оперативно ідентифікувати загрози через автоматизовані сценарії моніторингу;

– час реагування на інциденти (Mean Time to Respond, MTTR): ефективність SOAR визначається зменшенням часу, необхідного для нейтралізації інцидентів за допомогою автоматизованих процесів реагування;

– кількість хибнопозитивних спрацювань: зменшення цього показника вказує на покращення якості аналітики та налаштування сценаріїв оркестрації;

– рівень автоматизації процесів: частка інцидентів, що були оброблені автоматично без втручання людини, є ключовим індикатором зрілості впровадження SOAR;

– ефективність команд SOC (Security Operations Center): вимірюється через кількість інцидентів, які команда може обробити за одиницю часу, завдяки автоматизації [15].

Впровадження систем SOAR (Security Orchestration, Automation, and Response) у великих організаціях демонструє значне покращення показників кібербезпеки.

Наприклад, українська компанія Octava Defence, що спеціалізується на кібербезпеці, інтегрувала SOAR для обробки понад 5000 сповіщень на день. Це підвищило продуктивність аналітиків, об’єднавши інформацію з різних систем безпеки в єдиний інтерфейс, що дало змогу ефективніше розставляти пріоритети та швидше реагувати на інциденти, які потребують втручання людини [16].

Guardian Alarm - це компанія, яка використовує технології прогнозної аналітики для виявлення аномальної поведінки в системах безпеки, що є частиною їхньої стратегії впровадження SOAR. Це дозволяє їм проактивно реагувати на потенційні загрози та підвищувати загальний рівень безпеки [17].

Ці приклади підкреслюють ефективність впровадження SOAR у різних організаціях, що призводить до покращення показників кібербезпеки та оптимізації процесів реагування на інциденти.

Оцінка ефективності впровадження моделі SOAR (Security Orchestration, Automation, and Response) є багатовимірним завданням, що виходить за межі аналізу базових метрик, таких як середній час виявлення загроз (MTTD) чи середній час реагування на інциденти (MTTR). У сучасному ландшафті кібербезпеки, де загрози стають дедалі складнішим, динамічнішими та непередбачувішиим, критерії оцінювання мають охоплювати технічні, економічні, стратегічні та операційні аспекти [18].

Насамперед критично важливим є здатність системи SOAR адаптуватися до динамічних загроз. Це передбачає не лише швидкість реагування на відомі загрози, а й здатність до проактивного захисту від невідомих атак, таких як Zero-Day вразливості. У цьому контексті оцінюється здатність системи інтегрувати нові алгоритми виявлення, швидко оновлювати бази даних загроз і модифікувати сценарії автоматизації без зупинки операційної діяльності. Важливим аспектом є також підтримка постійної кореляції даних між різними джерелами в реальному часі, що дає змогу забезпечити своєчасне виявлення комплексних атак із багатовекторними сценаріями.

Другим ключовим аспектом оцінювання є рівень операційної інтеграції SOAR у загальну екосистему кібербезпеки організації. Ефективна інтеграція системи із такими рішеннями, як SIEM, EDR чи XDR, є основоположним фактором, оскільки вона визначає якість та швидкість передачі даних між компонентами безпеки. Крім того, важливим є забезпечення безшовної взаємодії між автоматизованими процесами та ручним втручанням аналітиків, що дає змогу мінімізувати людські помилки під час реагування на інциденти. Такий підхід забезпечує ефективну координацію міждисциплінарних команд та зменшує ризики невідповідності між різними підрозділами.

Економічна віддача від впровадження SOAR також потребує глибокого аналізу. Оцінка ROI (Returnon Investment) виходить за межі безпосередніх фінансових витрат на придбання та підтримку системи. Вона включає потенційні заощадження, пов'язані зі зниженням кількості збоїв, витрат на ліквідацію наслідків кіберінцидентів і, що важливо, зменшенням фінансових втрат від простоїв або витоків даних. Крім того, автоматизація рутинних завдань дає змогу оптимізувати роботу команд SOC (Security Operations Center), скорочуючи витрати на залучення додаткового персоналу та підвищуючи ефективність роботи існуючих ресурсів.

Ще одним важливим напрямом оцінювання є забезпечення відповідності системи SOAR нормативно-правовим вимогам. У сучасному регульованому середовищі, де ключовими аспектами діяльності є відповідність таким стандартам, як GDPR, HIPAA чи PCI DSS, SOAR має забезпечувати повну прозорість дій і можливість автоматичного створення детальних звітів про всі етапи обробки інцидентів. Це не лише полегшує процеси аудиту, а й підвищує довіру з боку внутрішніх і зовнішніх зацікавлених сторін [19].

SOAR-платформи мають бути оснащені функціоналом автоматичного документування всіх дій, пов'язаних із виявленням, аналізом і реагуванням на інциденти. Це включає:

– автоматизовану генерацію звітів: генерація звітів має охоплювати всі етапи обробки інцидентів, починаючи від отримання алертів і закінчуючи остаточним вирішенням інциденту. Звіти мають містити детальну хронологію дій, інформацію про відповідальних осіб, залучені ресурси та застосовані політики;

– спростування випадків "непрозорого реагування": завдяки прозорості SOAR можна зменшити ймовірність порушення регуляторних норм. Наприклад, автоматизовані playbooks можуть містити обов'язкові кроки з верифікації відповідності кожної дії регуляторним вимогам;

– інтеграція з системами управління ризиками: SOAR має інтегруватися з платформами GRC (Governance, Risk, and Compliance) для виявлення порушень та автоматизації процесів виправлення недоліків. Це дає змогу оцінити ризики ще до їх реалізації;

– протоколювання для аудиту: SOAR забезпечує безперервний моніторинг із записом всіх транзакцій і змін у системі. Такі протоколи є ключовими доказами відповідності, що зменшує навантаження під час аудитів та сприяє проходженню сертифікації [20, с. 59].

Останнім, але не менш важливим аспектом є оцінка користувацького досвіду (UX) та сприйняття системи співробітниками. Як показують дослідження, складний інтерфейс або недостатня зручність використання можуть стати бар'єром для ефективного впровадження навіть найпотужніших технологій. Тому важливими метриками є час, необхідний для навчання співробітників, і рівень їхньої задоволеності системою. Регулярний зворотний зв'язок із користувачами дає змогу виявити слабкі місця та вдосконалити функціональність платформи, роблячи її більш зручною для повсякденного використання.

Отже, розширена оцінка ефективності SOAR є комплексним процесом, що потребує врахування багатьох взаємопов'язаних факторів. Лише поєднання технічних, економічних, операційних і людських аспектів дає змогу сформувати цілісну картину ефективності впровадження цієї моделі в умовах сучасного кіберзагрозливого середовища.

Перспективи та вдосконалення моделі SOAR

Перспективи розвитку та вдосконалення моделі SOAR (Security Orchestration, Automation, and Response) пов'язані з інтеграцією інноваційних технологій, таких як штучний інтелект (AI) і машинне навчання (ML), які здатні забезпечити більш точне прогнозування загроз і динамічне налаштування сценаріїв автоматизації. У майбутньому SOAR може стати основою для створення автономних систем кіберзахисту, що поєднують здатність до самонавчання, міжплатформову інтеграцію та адаптацію до мультихмарних і гібридних середовищ. Такий підхід дозволить значно підвищити швидкість реагування на загрози, мінімізувати людський фактор і забезпечити безперервний моніторинг безпеки в умовах постійно змінюваного кіберландшафту.

Інтеграція з інтелектуальними технологіями

Інтеграція моделі SOAR (Security Orchestration, Automation, and Response) з інтелектуальними технологіями відкриває нові горизонти для підвищення ефективності кіберзахисту через використання штучного інтелекту (AI), автоматизованих систем навчання та великих даних (Big Data). Цей симбіоз дає змогу не лише оптимізувати існуючі процеси, а й створювати нові можливості для прогнозування та адаптації у динамічному середовищі загроз.

Штучний інтелект відіграє ключову роль у прогнозуванні інцидентів кібербезпеки завдяки здатності до аналізу величезних обсягів інформації в реальному часі. Зокрема, алгоритми машинного навчання можуть ідентифікувати аномальні патерни в мережевому трафіку, передбачати ймовірні вектори атак і пропонувати ефективні заходи реагування ще до настання інциденту. Наприклад, предиктивні моделі, побудовані на основі історичних даних і динамічних загрозових індикаторів, дають змогу створювати сценарії автоматизації, які проактивно запобігають атакам, знижуючи ризик їхньої ескалації.

Автоматизовані системи навчання та адаптації є важливим компонентом розширення функціональності SOAR. Їхня основна перевага полягає у здатності до самонавчання на основі нового досвіду. Це забезпечує динамічне оновлення сценаріїв автоматизації та політик реагування без необхідності ручного втручання. Наприклад, використання методів підкріплювального навчання дозволяє системі самостійно оптимізувати реагування на інциденти, базуючись на успішності попередніх дій. Крім того, такі системи здатні адаптуватися до нових середовищ і типів загроз, забезпечуючи безперервний захист навіть у мультихмарних і контейнеризованих інфраструктурах [21].

Роль великих даних у покращенні функцій SOAR є фундаментальною, оскільки вони надають платформу для створення високоточних моделей аналізу загроз. Використання Big Data забезпечує інтеграцію даних з різних джерел, таких як SIEM, EDR, XDR. Ці дані дають змогу створювати контекстуалізовані профілі загроз і проводити кореляційний аналіз, що мінімізує кількість хибнопозитивних спрацювань. Наприклад, глибокий аналіз поведінкових даних користувачів і пристроїв дає змогу виявляти складні атаки, які не можуть бути ідентифіковані за допомогою традиційних методів.

Уніфікація стандартів кібербезпеки

Гармонізація міжнародних стандартів кібербезпеки, таких як NIST Cybersecurity Framework і ISO / IEC 27001, є важливим аспектом для ефективного впровадження моделі SOAR (Security Orchestration, Automation, and Response). Ці стандарти забезпечують структуровану основу для створення, впровадження, моніторингу та вдосконалення процесів кіберзахисту. У контексті SOAR гармонізація стандартів дає змогу досягти уніфікації підходів до ідентифікації ризиків, автоматизації процедур реагування та управління безпекою. У табл. 1 наведено порівняльний аналіз ключових компонентів стандартів NIST та ISO / IEC 27001 із визначенням точок інтеграції з SOAR.

Таблиця 1

Порівняльний аналіз ключових компонентів стандартів NIST та ISO / IEC 27001 із визначенням точок інтеграції з SOAR

Категорія	NIST Cybersecurity Framework	ISO / IEC 27001	Інтеграція з SOAR
Управління ризиками	Оцінка ризиків на основі функцій: Identify, Protect, Detect, Respond, Recover	Систематичний процес управління ризиками (клаузи 6.1.2, 8.2)	SOAR використовує дані оцінки ризиків для пріоритизації автоматизованих заходів і сценаріїв реагування
Виявлення інцидентів	Функція Detect: орієнтація на моніторинг та виявлення аномалій	Вимога 12.4: моніторинг подій безпеки та реєстрація дій	Інтеграція SIEM і XDR для забезпечення кореляції даних і автоматичного виявлення загроз у рамках SOAR
Реагування на інциденти	Функція Respond: керування інцидентами та комунікація в реальному часі	Вимога 16: планування реагування на інциденти	SOAR автоматизує сценарії реагування, спрощує звітність і прискорює процес ескалації
Контроль доступу	Захист ресурсів через автентифікацію і сегментацію мережі (Protect)	Вимога 9: управління доступом до інформаційних активів	Автоматизація управління привілеями і моніторинг доступу через SOAR дають змогу уникати людських помилок
Безперервне вдосконалення	Функція Recover: моніторинг ефективності заходів безпеки	Вимога 10.3: впровадження циклу PDCA (Plan-Do-Check-Act)	SOAR забезпечує аналітику постінцидентного аналізу для вдосконалення політик і сценаріїв реагування

Гармонізація міжнародних стандартів NIST Cybersecurity Framework та ISO / IEC 27001 дає змогу створити надійну основу для впровадження SOAR у різноманітних організаціях. Інтеграція принципів і вимог цих стандартів із функціональністю SOAR забезпечує уніфікований підхід до ідентифікації ризиків, автоматизації реагування та вдосконалення процедур кіберзахисту. Завдяки цьому SOAR може виступати не лише як оперативне рішення, а й як стратегічний інструмент, який сприяє дотриманню нормативних вимог і підвищенню ефективності управління безпекою [22].

Важливо вказати, що використання API (Application Programming Interface) є ключовим компонентом інтеграції рішень у контексті побудови сучасних віртуальних мереж і забезпечення їхньої кібербезпеки. API слугують універсальним інструментом, який забезпечує взаємодію між різними платформами, сервісами та рішеннями, створюючи основу для оркестрації процесів і динамічного управління інфраструктурою. Завдяки стандартизованому доступу до функціоналу різноманітних систем API дозволяють SOAR інтегрувати різні джерела даних, такі як SIEM, EDR, XDR, та автоматизувати сценарії виявлення й реагування на інциденти. Цей підхід забезпечує не лише сумісність між продуктами різних виробників, а й дає змогу налаштовувати сценарії безпеки відповідно до специфічних вимог організації.

У платформо-орієнтованих підходах до побудови віртуальних мереж інтеграція API відіграє не менш важливу роль. Платформи для управління віртуальними мережами, такі як оркестратори контейнерів (наприклад, Kubernetes) чи хмарні сервіси (AWS, Azure, Google Cloud), надають розширений функціонал через API, що дає змогу SOAR інтегрувати ці компоненти в єдину екосистему. Це забезпечує гнучкість і масштабованість мережевих інфраструктур, одночасно знижу-

ючи складність їхньої експлуатації. Завдяки цьому підходу організації можуть ефективно управляти політиками доступу, динамічно адаптувати ресурси до змін у навантаженні та оптимізувати процеси моніторингу й аналізу безпеки.

Поєднання API-орієнтованих інтеграцій із платформо-орієнтованими підходами до побудови віртуальних мереж дає змогу реалізувати уніфіковану архітектуру управління, яка забезпечує високий рівень захисту в умовах децентралізованих і мультихмарних середовищ. Це не лише знижує операційні витрати, а й сприяє створенню більш адаптивних і стійких до загроз інфраструктур [23].

Майбутні дослідження та інновації

Зі зростанням доступності квантових обчислювальних систем постає необхідність адаптації моделей кібербезпеки, таких як SOAR, для роботи в нових обчислювальних середовищах. Квантові технології створюють як можливості, так і виклики: з одного боку, вони забезпечують швидке обчислення криптографічних функцій і складних алгоритмів, з іншого – загрожують безпеці сучасних шифрувальних протоколів. SOAR у квантовому середовищі має бути здатним інтегруватися з квантово-безпечними криптографічними алгоритмами (post-quantum cryptography), адаптувати сценарії реагування до швидко змінюваних загроз і використовувати потужність квантових обчислень для прогнозування атак. Ключовим завданням є розробка уніфікованих API та моделей інтерфейсу між квантовими й класичними системами, що дозволить SOAR працювати в гібридних середовищах.

Сучасні виклики кібербезпеки потребують адаптивних рішень, які можуть не лише реагувати на відомі загрози, а й навчатися на основі нових даних. Впровадження самонавчальних алгоритмів у SOAR дає змогу створити моделі, що здатні автоматично оптимізувати свої сценарії реагування на основі аналізу інцидентів. Завдяки методам глибокого навчання (deeplearning) і зміцненого навчання (reinforcement learning) такі алгоритми можуть не лише визначати закономірності у великомасштабних потоках даних, а й передбачати потенційні вразливості в реальному часі. Це забезпечує постійну адаптацію SOAR до нових векторів атак, зменшуючи залежність від людського втручання. Крім того, самонавчальні алгоритми сприяють автоматичному вдосконаленню процесів розподілу пріоритетів у реагуванні на інциденти, підвищуючи ефективність розслідування й усунення наслідків атак [24].

Цифрові двійники (digital twins) стали революційним інструментом для моделювання, тестування та вдосконалення складних інфраструктур у реальному часі. У контексті впровадження моделей SOAR (Security Orchestration, Automation, and Response) цифрові двійники не лише дають змогу проводити динамічне тестування, а й забезпечують ітеративний підхід до вдосконалення політик та механізмів безпеки на основі даних, зібраних у симуляційних середовищах.

Використання цифрових двійників у середовищах SOAR дає змогу:

– створювати багатовимірні моделі інфраструктури. Цифрові двійники відтворюють складні взаємодії між мережевими вузлами, користувацькими даними та інтегрованими кібербезпековими системами, що дає змогу аналізувати поведінку інфраструктури під впливом різноманітних факторів, включно з аномальним трафіком, атаками та збоями;

– емулювати реальні сценарії атак. Завдяки доступу до великих масивів даних та інтеграції з бібліотеками відомих кіберзагроз (наприклад, MITRE ATT&CK) цифрові двійники дають змогу моделювати складні багатовекторні атаки, такі як APT (Advanced Persistent Threats), відстежувати динаміку їхнього розвитку та оцінювати ефективність реагування систем SOAR;

– підвищувати ефективність алгоритмів машинного навчання. Тренування самонавчальних алгоритмів SOAR на основі реалістичних даних, отриманих у симуляційних середовищах цифрових двійників, дає змогу моделювати складні кореляційні залежності між джерелами атак, векторами компрометації та заходами протидії. Це сприяє вдосконаленню моделей прогнозування та зменшує кількість хибнопозитивних спрацювань;

– розробляти кастомізовані сценарії реагування. Цифрові двійники дають змогу інтерактивно тестувати та оптимізувати playbooks SOAR під специфічні сценарії атак. Наприклад, можна моделювати одночасні DDoS-атаки, фішингові кампанії та шифрувальні атаки з метою оцінки ефективності інтеграцій SOAR із мережевими брандмауерами, EDR / XDR системами та SIEM-платформами;

– аналізувати вплив масштабування інфраструктури на безпеку. Завдяки цифровим двійникам можна прогнозувати поведінку мережі під час збільшення кількості під'єднаних пристроїв, зростанні обсягу оброблюваних даних або впровадженні нових хмарних сервісів. Це дає змогу заздалегідь ідентифікувати вузькі місця та адаптувати SOAR до нових умов;

– верифікація та тестування у захищеному середовищі. Цифрові двійники забезпечують середовище, де можна проводити тестування нових сценаріїв автоматизації та політик безпеки без ризику для основної інфраструктури. Це передбачає перевірку відповідності стандартам, таким як ISO 27001 або NIST Cybersecurity Framework, а також аналіз ефективності реагування в умовах масштабних атак;

– прогнозування впливу змін. Моделювання змін у конфігураціях мережі або політик безпеки на основі цифрових двійників дає змогу оцінити можливий вплив цих змін на безпеку та загальну продуктивність. Наприклад, можна симулювати вплив заміни певного компонента мережі або оновлення систем безпеки;

– створення навчальних середовищ. Цифрові двійники забезпечують високореалістичні симуляції для підготовки фахівців із кібербезпеки. Тренувальні програми з використанням цифрових двійників дають змогу оператору SOAR відпрацьовувати складні сценарії інцидентів у реальних умовах, не ризикуючи продуктивним середовищем [25, 26].

Тому завдяки глибокій інтеграції з платформами SOAR цифрові двійники забезпечують новий рівень адаптивності та стійкості до кіберзагроз, скорочуючи час впровадження нових рішень та оптимізуючи витрати на безпеку. Цей підхід відкриває нові можливості для моделювання ризиків, розробки ефективних стратегій захисту та підвищення рівня кіберстійкості організацій.

Майбутні дослідження та інновації у сфері SOAR мають потенціал радикально трансформувати підходи до кібербезпеки. Адаптація до квантових середовищ, впровадження самонавчальних алгоритмів і використання цифрових двійників сприятимуть підвищенню автоматизації, ефективності та надійності моделей реагування, забезпечуючи сталий захист від зростаючих кіберзагроз.

Результати дослідження

Теоретичні основи моделі SOAR у кібербезпеці

Модель **SOAR** (Security Orchestration, Automation, and Response) є інтегрованим підходом до забезпечення кібербезпеки, що базується на взаємодії трьох фундаментальних компонентів (рис. 1):

– оркестрація (Orchestration): передбачає координацію різнорідних інструментів та процесів для створення єдиної, синхронізованої екосистеми. Завдяки стандартизованим інтерфейсам оркестрація забезпечує безперебійну взаємодію між рішеннями різних постачальників, включаючи інструменти моніторингу, управління доступом, аналізу загроз та реагування. Оркестрація мінімізує розриви між технологіями, даючи змогу реалізувати комплексний підхід до управління інцидентами;

– автоматизація (Automation): спрямована на зменшення обсягу рутинної роботи завдяки алгоритмізованим процесам обробки даних. Впровадження автоматизації дає змогу значно скоротити час виявлення та реагування на загрози (MTTD і MTTR), а також підвищити ефективність використання людських ресурсів. Приклади автоматизації включають автоматичну класифікацію інцидентів, запуск скриптів на основі попередньо визначених сценаріїв та генерацію звітів для подальшого аналізу;

– реагування (Response): передбачає оперативне прийняття рішень на основі інтегрованих даних та сценаріїв реагування. Реакція може бути частково або повністю автоматизованою, що дає змогу зменшити час між виявленням інциденту та його нейтралізацією. Реагування передбачає такі дії, як ізоляція скомпрометованих вузлів, блокування атакуючих IP-адрес, відновлення даних із резервних копій або інформування зацікавлених сторін [3, 4].

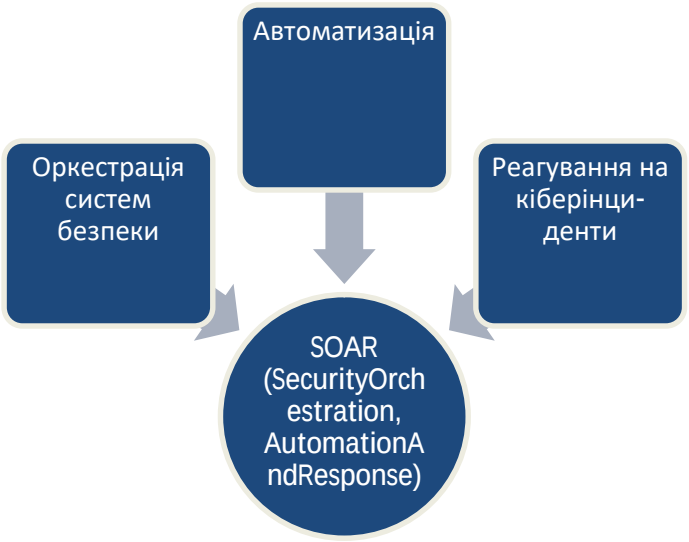

Рис. 1. Складові моделі SOAR

Зв'язок із іншими моделями кібербезпеки (SIEM, EDR, XDR)

SOAR є еволюційним доповненням та інтегратором інших кібербезпекових рішень, таких як **SIEM** (Security Information and Event Management), **EDR** (Endpoint Detection and Response) та **XDR** (Extended Detection and Response) [5, с. 62].

SIEM забезпечує централізований збір, кореляцію та аналіз подій із різних джерел у режимі реального часу. У контексті SOAR SIEM виконує функцію джерела даних, постачаючи інформацію для автоматизованого аналізу та реагування.

EDR зосереджений на захисті кінцевих точок, виявленні та реагуванні на загрози. SOAR використовує дані, отримані EDR, для координації дій між кінцевими точками та іншими компонентами інфраструктури.

XDR, як розширена модель виявлення, інтегрує дані не лише з кінцевих точок, а й з мережевих пристроїв, хмарних сервісів тощо. SOAR доповнює XDR механізмами автоматизації реагування, підвищуючи ефективність боротьби з багатокомпонентними атаками.

Тож SOAR не замінює зазначені рішення, а є їхнім об'єднавчим каркасом, забезпечуючи масштабованість, інтеграцію та динамічне управління кіберзахистом.

Візуалізація моніторингу безпеки на основі SOAR (Security Orchestration, Automation, and Response) є ключовим компонентом для ефективного управління кібербезпекою віртуальних мереж. Вона дає змогу організаціям автоматизувати процеси збору, аналізу та реагування на інциденти, що виникають у реальному часі. Завдяки інтеграції різних інструментів та платформ безпеки в єдину екосистему SOAR забезпечує швидке виявлення загроз, їх оперативну класифікацію та прийняття рішень без необхідності втручання людини. Візуалізація в такому контексті дає змогу створювати інтуїтивно зрозумілі дашборди, які відображають поточний стан безпеки мережі, забезпечують моніторинг активностей та дають змогу приймати обґрунтовані рішення щодо подальших дій для зменшення ризиків і запобігання загрозам (рис. 2) [6].

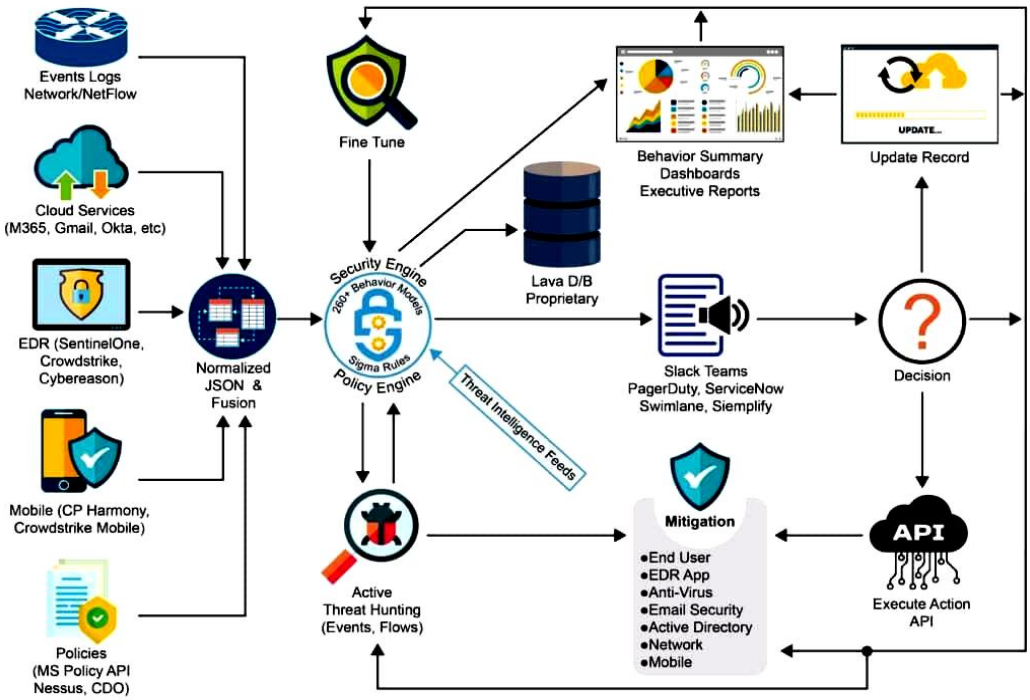

Рис. 2. Візуалізація моніторингу безпеки на основі SOAR

Впровадження SOAR у віртуальних мережах базується на архітектурному підході, який враховує специфіку децентралізованих і динамічних середовищ:

1. Рівень збору даних: передбачає інтеграцію з агентами моніторингу, журналами подій, API хмарних сервісів та мережевими сенсорами. У цьому контексті використовується концепція data lake для консолідації великих обсягів даних із різних джерел.

2. Рівень обробки даних: побудований на основі платформ аналізу великих даних, що включають машинне навчання та механізми кореляції для виявлення аномалій. Застосування когнітивних алгоритмів дає змогу ідентифікувати складні атаки на основі поведінкових патернів.

3. Рівень реагування та управління: реалізується через централізовану консоль управління, яка дає змогу автоматизувати запуск сценаріїв реагування, формувати аналітичні звіти та забезпечувати зворотний зв’язок для постійного вдосконалення моделей виявлення [7, с. 53].

Архітектура SOAR у віртуальних мережах спрямована на динамічну адаптацію до змін у конфігурації середовища, забезпечуючи одночасно високу швидкість реагування та збереження системної цілісності. Це робить модель особливо ефективною в умовах мультихмарних і гібридних середовищ.

Класифікація загроз у віртуальних мережах

Віртуальні мережі, що слугують основою для сучасних децентралізованих інфраструктур, схильні до широкого спектра загроз, які можна класифікувати за трьома основними категоріями [8]:

1. Мережеві атаки:

– DDoS-атаки (Distributed Denial of Service): спрямовані на перевантаження мережевих ресурсів з метою тимчасового або повного порушення доступу до систем. У віртуальних мережах такі атаки можуть ускладнюватися через масштабованість та еластичність середовищ:

– атаки на рівні протоколів: експлуатація вразливостей у протоколах маршрутизації (наприклад, BGP hijacking) або віртуалізації (наприклад, VXLAN);

– сканування мережі та підбір конфігурацій: дії, спрямовані на ідентифікацію слабких вузлів через несанкціоноване сканування портів, служб і версій ПЗ.

2. Злом даних:

– експлуатація вразливостей доступу: атаки, пов’язані зі зломом облікових записів або використанням вразливих механізмів автентифікації (наприклад, brute force або credential stuffing);

– крадіжка даних: несанкціонований доступ до конфіденційної інформації, що зберігається у віртуальних сховищах, як-от дані користувачів, бізнес-дані або секретну інформацію про конфігурації мережі;

– атаки на API: специфічні для хмарних середовищ методи атак, спрямовані на отримання контролю над сервісами через зловживання публічними інтерфейсами програмування.

3. Внутрішні порушення:

– зловмисні дії інсайдерів: викрадання даних, порушення цілісності конфігурацій або впровадження шкідливого програмного забезпечення працівниками, що мають доступ до критичних ресурсів;

– ненавмисні помилки: дії користувачів, спричинені недостатнім рівнем підготовки або розумінням безпеки, наприклад, неправильно налаштовані правила доступу або публікація конфіденційних даних у загальнодоступних репозиторіях;

– компрометація привілейованих облікових записів: спрямоване використання доступу адміністраторів для отримання контролю над віртуальним середовищем.

На рис. 3 зображено розподіл найпоширеніших типів кібератак на основі глобальних даних за 2024 рік [9].

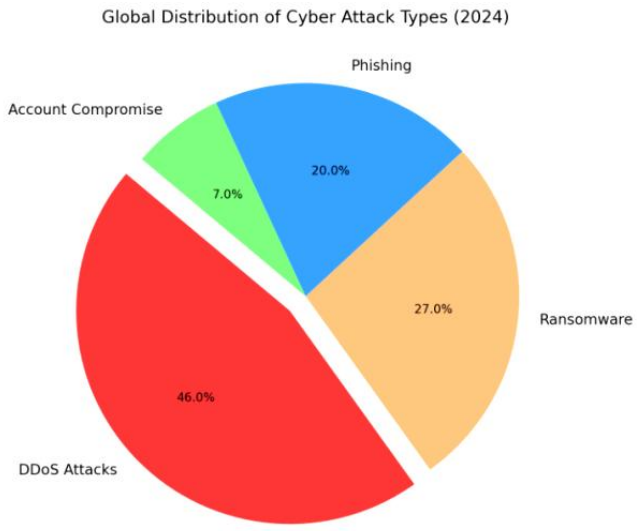

Рис. 3. Розподіл найпоширеніших типів кібератак

Потрібно зазначити, що децентралізовані середовища характеризуються швидкою зміною топології мережі. Автоматичне створення та видалення ресурсів ускладнює моніторинг і виявлення загроз у реальному часі. Це особливо актуально для контейнерних оркестраторів, таких як Kubernetes, де масштабованість та еластичність додають додаткових викликів для забезпечення безпеки.

Розширена поверхня атаки є наслідком використання різних постачальників хмарних послуг та їх API. У таких умовах недостатньо захищені точки інтеграції між платформами часто стають ключовими вразливими місцями, які зловмисники можуть експлуатувати для несанкціонованого доступу або компрометації ресурсів.

Управління доступом до ресурсів у децентралізованих середовищах є складним завданням. Часто виникають ситуації, коли права доступу надаються надмірно через помилки конфігурації або недостатньо надійні механізми автентифікації. Це створює ризики як зовнішніх, так і внутрішніх загроз, що потребують постійного моніторингу та оптимізації політик доступу.

Популярність контейнерних технологій, таких як Docker і Kubernetes, зробила їх привабливою мішенню для зловмисників. Вразливості в контейнерних образах або оркестраторах можуть бути використані для виконання несанкціонованого коду, розширення привілеїв або впровадження шкідливих компонентів у критичну інфраструктуру. Це підкреслює необхідність регулярного аудиту контейнерів та їх конфігурацій.

У табл. 2 презентовано основні метрики, які використовуються для оцінки ризиків у контексті віртуальних мереж. Вона містить показники, що враховують ймовірність загрози, її вплив на систему та інтегральний рівень ризику. Такий підхід дає змогу формалізувати процеси управління безпекою та пріоритизувати заходи реагування [10, 11].

Таблиця 2

Метрики оцінки ризиків у контексті віртуальних мереж

Метрика	Опис	Методологія розрахунку	Приклад використання
Ймовірність виникнення загрози (Threat Likelihood)	Вірогідність реалізації певної загрози у заданому середовищі	Використання історичних даних про інциденти, CVSS для оцінки вразливостей	Прогнозування ймовірності DDoS-атаки на основі аналізу минулих атак на подібну інфраструктуру
Потенційний вплив (Impact Assessment)	Ступінь шкоди, яка може бути заподіяна конфіденційності, цілісності та доступності	Вимірювання впливу на критичні сервіси, обсяг втраченої інформації	Оцінка наслідків компрометації облікового запису адміністратора в хмарному середовищі
Час виявлення загрози (Mean Time to Detect, MTTD)	Середній час, необхідний для виявлення загрози після її виникнення	Моніторинг показників SIEM та логів	Порівняння часу виявлення аномалії у контейнерному середовищі до й після впровадження SOAR
Час реагування (Mean Time to Respond, MTTR)	Середній час, необхідний для нейтралізації загрози після її виявлення	Вимірювання часових інтервалів між активацією інструментів реагування	Аналіз ефективності автоматизованого реагування під час спроби злому через API
Загальний ризик (Risk Score)	Інтегральний показник, що враховує ймовірність та вплив загрози	Використання матриць ризиків або алгоритмів машинного навчання	Розрахунок пріоритетності усунення уразливості на основі потенційних втрат та частоти її експлуатації

Подібна класифікація дає змогу оптимізувати процес управління ризиками, виділяючи ресурси на вирішення найкритичніших проблем.

Висновки

Отже, дослідження підкреслює фундаментальну роль моделі SOAR (Security Orchestration, Automation, and Response) у сучасній кібербезпеці, зокрема в контексті захисту віртуальних мереж. Модель SOAR демонструє здатність інтегрувати різнорідні системи безпеки, автоматизувати складні процеси реагування на загрози та значно знижувати залежність від людського фактора. Використання цієї моделі сприяє суттєвому скороченню часу виявлення та реагування на інциденти, підвищенню ефективності управління ризиками та вдосконаленню механізмів захисту в умовах динамічних мультихмарних середовищ.

Крім того, дослідження засвідчує перспективність інтеграції SOAR із сучасними технологіями, такими як штучний інтелект, великі дані та автоматизовані системи навчання. Такий підхід забезпечує високий рівень адаптивності та ефективності, відкриваючи нові горизонти у прогно-

зуванні загроз та вдосконаленні інструментів реагування. Завдяки цьому SOAR стає не лише ефективним операційним інструментом, а й стратегічним рішенням для забезпечення кібербезпеки в умовах постійно зростаючої складності атак.

Подальші дослідження мають бути спрямовані на адаптацію SOAR до викликів квантових обчислень, які здатні суттєво змінити кіберзагрозливий ландшафт. Розробка інтеграційних механізмів для квантово-безпечної криптографії та гібридних середовищ стане важливим кроком у цьому напрямі. Також актуальним залишається впровадження самонавчальних алгоритмів, які можуть підвищити автономність моделі, та розвиток цифрових двійників, що сприятимуть безпечному тестуванню сценаріїв кіберзахисту без ризику для основної інфраструктури. Ці напрями досліджень сприятимуть формуванню нової генерації рішень у сфері кібербезпеки, які відповідатимуть викликам майбутнього.

Список літератури

1. *Mykhaylova O., Fedynyshyn T., Datsiuk A., Fihol B., Hulak H. Mobile application as a critical infrastructure cyberattack surface. In CEUR Workshop Proceedings. 2023. Vol. 3550. Pp. 29–43. DOI: https://doi.org/10.15587/978-617-8360-12-2.*
2. *Shevchuk D., Harasymchuk O., Partyka A., Korshun N. Designing secured services for authentication, authorization, and accounting of users (short paper). In CPITS II 2023. Pp. 217–225. DOI: https://doi.org/10.28925/2663-4023.2023.20.272282.*
3. *Barnes S. SOAR platforms and compliance automation. Journal of Cyber Law. 2023. 18(2). 23–34.*
4. *White J. Automating security workflows with SOAR. Cyber Defense Magazine. 2022. 7(2). 41–50.*
5. *Kotlyarov O. Yu., Bortnik L. L. Comparative analysis of modern virtual network protection systems and their methodologies. Modern Information Protection. 2024. 4(60). 60–72. DOI: https://doi.org/10.31673/2409-7292.2024.040007.*
6. *Johnson K. The impact of automation in security operations centers. Cybersecurity Review. 2022. 15(2). 33–45.*
7. *Anderson J., Parker R. The role of SOAR platforms in modern SOCs. Journal of Cybersecurity Automation. 2023. 12(3). 45–60.*
8. *Ocheretny S. O., Kryzhanovsky V. G. Intrusion detection and prevention systems: the most successful practices. 2024. URL: http://cit-journal.com.ua/index.php/cit/article/view/209 https://jpasmd.donnu.edu.ua/article/view/ 14833 (Accessed: 4 January 2025).*
9. *Octava (n.d.). We process 5000+ cybersecurity alerts per day. URL: https://octava.ua/en/cyber-security/ (Accessed: 10 January 2025).*
10. *Korobeinikova T. I., Tsar O. O. Analysis of modern open intrusion detection and prevention systems. Grail of Science. 2023. (27). 317–325. DOI: https://doi.org/10.36074/grail-of-science.12.05.2023.050.*
11. *Susukailo V. V. Using the DEVSECOPS approach to analyze modern information security threats. Electronic Professional Scientific Publication "Cybersecurity: Education, Science, Technology". 2021. 2(14), 26–35. DOI: https://doi.org/10.28925/2663-4023.2021.14.2635.*
12. *Smith D. How SOAR platforms enhance incident response. Information Security Journal. 2023. 11(5). 78–84.*
13. *Kim J. Orchestrating multi-vendor security solutions with SOAR. Cybersecurity Automation Journal. 2023. 12(4). 70–78.*
14. *Green A. SOAR and threat intelligence integration. Journal of Threat Intelligence. 2023. 6(1). 12–20.*
15. *Mtakai N. J. (n.d.). The role of security orchestration, automation, and response (SOAR) platforms. LinkedIn. URL: https://www.linkedin.com/pulse/role-security-orchestration-automation-response-soar-platforms-4fncf (Accessed: 9 January 2025).*
16. *Koloshchuk M. S., Dyachuk O. Yu., Okunkova O. O., Pirog O. V. Artificial intelligence tools for penetration testing automation. Technical Engineering. 2025. 2(94). 121–128. DOI: https://doi.org/10.26642/ten-2024-2(94)-121-128.*
17. *Liga.net. (n.d.). AI risk: how artificial intelligence shapes new horizons of corporate security. URL: https://mindblastai.com/data-leaks-in-ai-risks-and-controversies/ (Accessed: 9 January 2025).*
18. *Black P. The role of SOAR in mitigating human error. Journal of Information Security. 2023. 13(3). 29–38.*
19. *Buryachok V. L. et al. Network infrastructure security technologies: Textbook. Kyiv : KUBG, 2019.*
20. *Patel N. Automating incident response with SOAR. Computer Security Review. 2022. 14(6). 53–62.*

21. Kushnerev O., Pozovna I., Sokol V. Influence of neuronal networks on development cybersecurity in the conditions of regulatory changes. Ukrainian Scientific Journal of Information Security. 2024. 30(2). 261–269. DOI: https://doi.org/10.18372/2225-5036.30.19238.

22. Masood S., Anwar Z. A comprehensive survey on SOAR platforms in cybersecurity. Computers & Security. 2024. 133. DOI: https://doi.org/10.1016/j.cose.2024.102892.

23. Prates L., Faustino J., Silva M., Pereira R. DevSecOps metrics. In Information Systems: Research, Development, Applications, Education Springer International Publishing, 2019. Pp. 77–90. DOI: https://doi.org/10.1007/978-3-030-29608-7_7.

24. Chakravarty Sh. (n.d.). How SOAR transforms security operations: A real-world case study. SANS Institute. URL: https://www.sans.org/blog/how-soar-transforms-security-operations-a-real-world-case-study/ (Accessed: 5 January 2025).

25. Selvidge J. (n.d.). Understanding the role of SOAR in business cybersecurity operations. SecureTrust. URL: https://securetrust.io/blog/understanding-the-role-of-soar-in-business-cybersecurity-operations/ (Accessed: 11 January 2025).

26. Lee S. SOAR platforms: A new era in cybersecurity automation. Technology Today. 2023. 19(4). 102–109.

OVERVIEW OF THE FUNDAMENTAL MODEL OF SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE IN THE CONTEXT OF CYBERSECURITY OF VIRTUAL NETWORKS

O. Y. Kotliarov, L. L. Bortnik

Lviv Polytechnic National University,
Department of Information Protection

The aim of this study is a comprehensive analysis of the fundamental SOAR (Security Orchestration, Automation, and Response) model in the context of cybersecurity for virtual networks. The paper presents a synthesis of the core concepts of orchestration, automation, and response, which are critical elements of modern approaches to risk management and information system protection. Particular attention is paid to the integration of SOAR with existing cybersecurity technologies such as SIEM, EDR, and XDR, enabling the creation of a unified security ecosystem that ensures rapid threat detection, classification, and response.

The study examines the classification of threats inherent to decentralized and multi-cloud environments, including protocol-level attacks, data breaches, and insider threats, while emphasizing specific challenges such as network configuration dynamics and the scalability of security solutions. A comparative analysis of SOAR's compliance with international cybersecurity standards (NIST, ISO 27001) demonstrates its ability to harmonize approaches and automate compliance procedures with regulatory requirements.

The research also covers prospective directions for SOAR development, including the implementation of artificial intelligence and self-learning algorithms for adaptive threat management, the use of digital twins to simulate security scenarios, and adaptation to the challenges of quantum computing. Additionally, the role of big data in enhancing SOAR functionality is highlighted, particularly in reducing false positives and identifying multi-vector attacks.

The results of this study have an applied nature and are aimed at improving cybersecurity tools to ensure comprehensive protection of virtualized environments. It is concluded that the SOAR model is a key component in forming strategic approaches to the protection of information assets in the context of evolving cyber threats.

Keywords: Cybersecurity, SOAR, automation, multi-cloud environments, risk management, security standards, virtual networks, network traffic.