



Іван ОПІРСЬКИЙ, д-р техн. наук, проф.

ORCID ID: 0000-0002-8461-8996

e-mail: ivan.r.opirskyi@lpnu.ua

Національний університет "Львівська політехніка", Львів, Україна

Соломія ЯВОРІВСЬКА, студ.

ORCID ID: 0009-0002-0018-6231

e-mail: solomiia.yavorivska.kb.2023@lpnu.ua

Національний університет "Львівська політехніка", Львів, Україна

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ SOAR ЯК ГОЛОВНОГО ІНСТРУМЕНТУ ДЛЯ ПРИСКОРЕННЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Вступ. Інтенсивний розвиток кіберзагроз і зростання їхньої складності в сучасному цифровому середовищі створюють критичні виклики для центрів операційної безпеки (SOC), які потребують нових підходів до автоматизації та оркестрації процесів кібербезпеки. Однією з ключових проблем сучасних SOC є необхідність оброблення величезних обсягів інформації про загрози, швидкого реагування на інциденти та координації дій між різними системами безпеки за обмежених людських ресурсів. У контексті дефіциту кваліфікованих фахівців із кібербезпеки особливої актуальності набувають платформи SOAR (Security Orchestration, Automation, and Response), які можуть автоматизувати рутинні процеси без втрати якості аналізу. Застосування інтегрованих механізмів оркестрації, зокрема й автоматизація реагування на фішинг, координація між SIEM-системами й управління інцидентами, формують основу сучасного підходу до ефективного функціонування SOC.

Методи. Проведено систематичний аналіз сучасних методів упровадження SOAR-систем у центрах операційної безпеки, зокрема і в контексті інтеграції з існуючими SIEM-платформами. Використано методи порівняльного аналізу, моделювання сценаріїв загроз, практичного тестування автоматизованих робочих процесів та оцінювання ефективності різних стратегій упровадження. Особливу увагу приділено аналізу ключових показників ефективності, таких як скорочення середнього часу виявлення загроз (MTTD) та реагування на них (MTTR), автоматизації процесів класифікації інцидентів та інтеграції з джерелами розвідки загроз. Для кожного з підходів оцінено складність упровадження, вимоги до кваліфікації персоналу, економічну ефективність і сумісність з архітектурою існуючих SOC.

Результати. Аналіз показав, що найефективнішим підходом до оптимізації SOC є поєднання SOAR-платформ із традиційними SIEM-системами у формі взаємодоповнюючої екосистеми. Наприклад, використання автоматизованих playbooks для реагування на фішинг суттєво скорочує час реакції з годин до хвилин, тоді як інтеграція з системами Threat Intelligence унеможливорює пропуск критичних індикаторів компрометації. Доведено, що комбінування автоматизації рутинних завдань із людським контролем стратегічних рішень значно підвищує продуктивність аналітиків SOC і точність виявлення справжніх загроз. Водночас упровадження SOAR вимагає ретельного планування та поетапного підходу, особливо для організацій з обмеженими ресурсами. Визначено оптимальні стратегії впровадження залежно від розміру організації, рівня зрілості процесів кібербезпеки та наявності кваліфікованого персоналу.

Висновки. Оптимізація роботи центрів операційної безпеки через упровадження SOAR-технологій вимагає системного і комплексного підходу, який враховує як технічні, так і організаційні аспекти. Комбінування автоматизації з людським досвідом дозволяє досягти високого рівня ефективності без втрати контролю над критичними процесами безпеки. Результати дослідження можуть бути використані для побудови інтегрованих систем кібербезпеки з урахуванням обмежених ресурсів малих і середніх організацій. Крім техніко-економічних аспектів, підкреслюється важливість поетапного впровадження, навчання персоналу та постійного вдосконалення автоматизованих сценаріїв відповідно до еволюції кіберзагроз. Системне впровадження SOAR-підходів забезпечить підвищення ефективності SOC навіть в умовах зростання кількості та складності кіберінцидентів.

Ключові слова: SOAR, SOC, кібербезпека, автоматизація реагування на інциденти, SIEM, оркестрування загроз, MTTD, MTTR, інтеграція інструментів безпеки, документація інцидентів, аналітика загроз, оптимізація SOC.

Вступ

Розслідування в центрах операційної безпеки (SOC) втомлюють, адже вони залежать від ручних дій для запитів до різних джерел даних, накладання відповідних журналів, кореляції даних в інформацію, а потім документування результатів у системі квитків. Інструменти оркестрації, автоматизації та реагування на загрози безпеки (SOAR) – це порівняно нова технологія, яка обіцяє за відповідного налаштування збирати, фільтрувати і відображати необхідну різноманітну інформацію, автоматизувати багато звичайних завдань, що без потреби забирають час аналітиків SOC, полегшити співпрацю SOC і підвищити ефективність та злагоженість роботи SOC.

Операційні центри безпеки – це частина команди інформаційних технологій підприємства, яка відповідає за захист організації від кіберзагроз. Сучасні SOC використовують широкий спектр датчиків, які генерують величезну кількість журналів аудиту (напр., журнали операційної системи з робочих хостів і серверів, мережеві потоки з роутерів, комутатор) канали розвідки (напр., звіти про сканування вразливостей, інформація про шкідливе програмне забезпечення) і сповіщення (напр., від антивірусних програм (AV) і систем виявлення мережових вторгнень (NIDS) на кінцевих точках). Більшість SOC оснащено системою управління інформацією та подіями безпеки (SIEM), яка об'єднує ці різноманітні потоки даних на централізованій платформі та надає конфігуровані інформаційні панелі й інтерфейси запитів для моніторингу даних, а також для відсіювання, сортування та пошуку артефактів з усієї мережі. Попри те, що системи SIEM забезпечують централізований збір та оброблення подій інформаційної безпеки, значне навантаження, пов'язане з аналізом великих обсягів даних із різноманітних джерел, усе ще покладається на фахівців центру моніторингу безпеки. Зокрема, аналітики й інженери повинні виконувати сортування значної кількості журналів подій, визначати, які з них потребують подальшого аналізу, встановлювати взаємозв'язки між різними сповіщеннями та приймати рішення щодо подальших дій у відповідь на виявлені інциденти.



Інструменти оркестрування, автоматизації та реагування на загрози безпеці (SOAR) представляють собою відносно нову технологію, яка намагається автоматизувати багато поширених ручних завдань із метою підвищення ефективності й узгодженості, і, як наслідок, безпеки. Якщо подивитись дані, які дає компанія Gartner (Гартнер) про SOAR, у своєму звіті про роботу, інструмент SOAR дозволяє "організаціям отримувати вхідні дані з різних джерел і застосовувати робочі процеси, узгоджені з процесами і процедурами, підвищуючи ефективність і узгодженість роботи людей і процесів". Основна відмінність між інструментом SOAR і SIEM полягає в тому, що інструменти SOAR мають конфігуровані робочі процеси або сценарії, які направляють аналітиків і автоматизують багато дій із розслідування і реагування на інциденти, в той час як основна функція інструменту SIEM полягає в широкому зборі даних і запитах. Існує певне дублювання, наприклад, обидва інструменти вимагають і полегшують отримання різноманітних даних і забезпечують налаштовану візуалізацію даних, зокрема й інформаційні панелі в реальному часі.

Інструменти SOAR мають на меті зробити операції з безпеки ефективнішими за рахунок автоматизації загальних завдань, визначення пріоритетів, кореляції і доповнення з допомогою вхідних сповіщень (напр., із розвідувальними даними про загрози), полегшення комунікації і співпраці між і всередині SOC, а також більш послідовними за рахунок надання уніфікованого, зручного інтерфейсу, за допомогою якого аналітики взаємодіють із розширеними даними і сповіщеннями, а також за рахунок використання сценаріїв для стандартизації процедури виявлення загрози.

Одними з ключових проблем у впровадженні SOAR є складність інтеграції, дефіцит кваліфікованих фахівців і нечітке розмежування функцій між SOAR і SIEM. По-перше, адаптація SOAR вимагає глибокого планування, ретельного налаштування сценаріїв автоматизації та постійного обслуговування, що ускладнює його впровадження, особливо для малих команд з обмеженими ресурсами. По-друге, незважаючи на те, що автоматизація через SOAR стає критичною через дефіцит спеціалістів із кібербезпеки, залишається недостатньо дослідженим, як максимізувати ефективність цих інструментів в умовах обмеженого персоналу, щоб вони не перетворилися на додаткове навантаження замість справжнього полегшення роботи SOC. По-третє, через нечітке розуміння ролей SOAR і SIEM організації часто стикаються з неефективним використанням обох систем, що призводить або до дублювання функцій, або до марних витрат, коли одна система використовується не повною мірою через неправильну інтеграцію з іншою. Ці фактори разом ускладнюють процес упровадження SOAR і можуть знизити його потенційну користь, якщо не будуть враховані на етапі планування.

Проблема дослідження полягає в тому, щоб зрозуміти, як найкраще впроваджувати SOAR-системи в SOC, особливо для невеликих компаній з обмеженим бюджетом і нестачею фахівців. Головні труднощі – це складне налаштування системи, нестача кваліфікованих працівників для її обслуговування, а також відсутність зрозумілих способів оцінити, чи дійсно SOAR покращує безпеку. Дослідження має допомогти знайти золоту середину між автоматизацією і роботою людей, а також запропонувати простий план упровадження SOAR для малого бізнесу.

Метою цього дослідження є аналіз особливостей упровадження SOAR-систем у центрах операційної безпеки для оптимізації реагування на кіберінциденти, з акцентом на інтеграцію із SIEM-платформами й автоматизацію рутинних процесів. З огляду на зростання складності загроз, таких як фішинг, підозрілі автентифікації та вразливості сертифікатів, необхідно розробити рекомендації щодо поетапного впровадження SOAR для організацій з обмеженими ресурсами, з метою скорочення MTTD та MTTR.

Для досягнення цієї мети передбачено розв'язання таких завдань:

- Проаналізувати сучасні випадки застосування SOAR-систем у кібербезпеці.
- Дослідити роль SOAR у центрі операційної безпеки (SOC) та їх вплив на ефективність роботи.
- Визначити оптимальні умови для впровадження SOAR-систем, з урахуванням обмежених ресурсів.
- Виявити ключові критерії ефективності SOAR у контексті зростаючої кількості кіберзагроз.
- Розробити рекомендації щодо впровадження SOAR-систем для підвищення продуктивності SOC.

Огляд літератури. У сучасному світі кібербезпеки, де атаки стають дедалі складнішими й частішими, ключовим фактором ефективного захисту стає поєднання автоматизації, штучного інтелекту та людського контролю (Seeton). Автоматизація реагування на інциденти (рішення SOAR), (2025).

Suchsmita Chatterjee у роботі "Using SIEM and SOAR for Real-Time Cybersecurity Operations" (Chatterjee, 2020) докладно пояснює, як об'єднання систем SIEM і SOAR дає змогу значно скоротити час виявлення загроз і реагування на них. SIEM (система управління інформацією та подіями безпеки) відповідає за збір і аналіз логів з усіх джерел у мережі, а SOAR (платформа оркестрації та автоматизації реагування) дає змогу автоматично виконувати дії у відповідь – наприклад, блокувати підозрілу IP-адресу чи запускати сценарій реагування на фішинг. Такий підхід зменшує навантаження на аналітиків і дозволяє команді безпеки зосередитися на складніших загрозах, які потребують людського втручання.

Із прикладом упровадження автоматизації саме в телекомунікаційній галузі можна ознайомитися у дослідженні Noshi, & Blaser (2024). Автор акцентує увагу на тому, що телекомунікаційні мережі є одними з найбільш складних і водночас вразливих до атак – зокрема, через використання застарілих протоколів і мільйони IoT-пристроїв. Він показує, як завдяки впровадженню SOAR-сценаріїв можна майже миттєво виявити й нейтралізувати загрозу, не чекаючи втручання людини. Наприклад, якщо у системі помічено аномальну активність у певному регіоні – SOAR може автоматично повідомити службу безпеки, виконати попередній аналіз, та, у разі підтвердження, обмежити доступ до вразливого сегменту мережі.

Дуже практичний погляд на автоматизацію реагування подає українська компанія Seeton у своєму матеріалі про впровадження SOAR (Sharma, & Spunda, 2025). Тут описано реальні кейси: як система автоматично обробляє фішингові листи, блокує заражені хости або взаємодіє із зовнішніми Threat Intelligence платформами. Важливо, що автори не лише описують технічні переваги, а й акцентують увагу на необхідності правильного проєктування процесів – створення playbooks, визначення критеріїв спрацювання, навчання персоналу. Автоматизація без розуміння процесів не працює – це головний висновок із цього джерела.



Однак навіть найсучасніші технології залишаються під контролем людини, і саме людський фактор часто стає причиною помилок.

У книзі "Behind Human Error" (Woods et al., 1994) розглянуто, чому фахівці припускаються помилок під час роботи з технічними системами. У випадку SOC аналітики часто стикаються з перевантаженням інформацією, втомою, стресом. Це призводить до пропущених інцидентів або неправильного реагування. Автори стверджують, що автоматизація повинна не замінити людину, а допомагати їй – наприклад, через фільтрацію тривог, нагадування, підказки. У такий спосіб технологія стає партнером, а не конкурентом фахівця.

У дослідженні "Testing SOAR tools in use" (Bridges et al., 2025), проведеному великою групою авторів, здійснено глибоку перевірку реальної ефективності інструментів SOAR у практичному середовищі. Основна увага приділялася тому, як саме такі платформи працюють у різних сценаріях, наскільки вони сумісні з іншими системами і чи відповідають вони очікуванням користувачів у реальному часі. Автори виявили, що попри гучні обіцянки автоматизації, деякі SOAR-рішення вимагають значного налаштування, добре описаних сценаріїв реагування та глибокого розуміння контексту загроз. Також у дослідженні зазначено, що без якісних джерел даних (SIEM, Threat Intelligence, внутрішні логи) платформи SOAR не можуть ефективно виконувати свої функції. Отже, інструменти SOAR не є "чарівною таблеткою", а скоріше потужним доповненням до налагодженого процесу кіберзахисту. Особливу увагу автори приділяють необхідності тестування платформ перед їх повноцінним впровадженням, адже не всі вони однаково добре працюють у кожній організації.

Усі ці джерела разом формують цілісну картину: кібербезпека нині – це не лише про інструменти, а про їхнє грамотне поєднання з людським досвідом. Автоматизація, якщо вона правильно налаштована, дає змогу не лише зекономити час, а і зменшити кількість помилок, підвищити точність рішень і зробити команди безпеки ефективнішими. Проте людина все ще залишається в центрі цих процесів, а технології повинні лише посилювати її можливості, а не повністю їх замінити.

Методи

В роботі використано методи аналізу, які включають систематичне картування наукових публікацій із SOAR-технологій та операційної безпеки, теоретичне моделювання процесів автоматизації реагування на кіберінциденти, порівняльний аналіз ефективності SIEM- та SOAR-систем, емпіричне тестування сценаріїв виявлення фішингу та підозрілої активності користувачів, а також оцінювання критеріїв успішності впровадження платформ оркестрації в SOC з обмеженими ресурсами, що дозволило досягти комплексного розуміння принципів оптимізації центрів операційної безпеки через інтеграцію автоматизованих систем реагування на кіберзагрози.

Результати

У SOC посадові функції швидко змінюються. Традиційно SOC розподіляють посади за рівнями, починаючи з рівня досвіду й обов'язків, необхідних для кожної з них (рис. 1) (Brewer, 2019). Робочі місця 1-го рівня є початковими, а робочі місця 3-го рівня потребують всебічних знань.

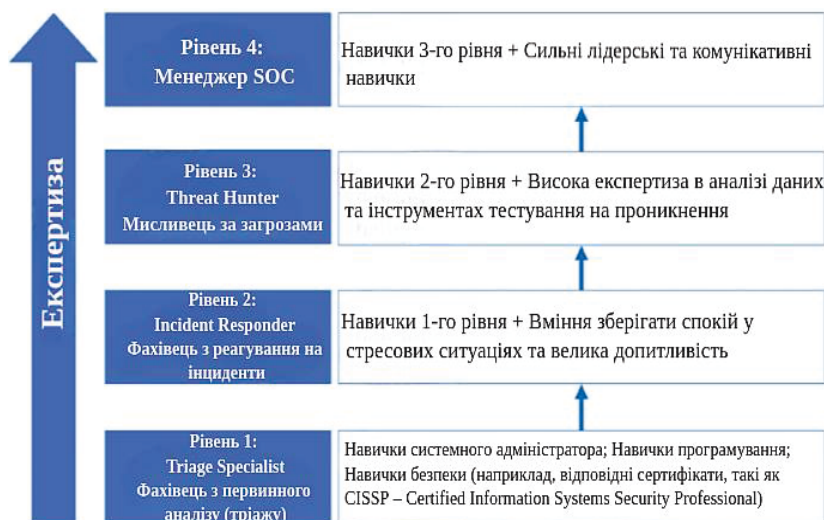


Рис. 1. Ролі в сучасному SOC

Аналітик Tier 1 – часто відомий як аналітик із кібербезпеки або спеціаліст із кібероперацій, відстежує вхідні повідомлення, перевіряє, чи дійсно стався інцидент. Якщо стався справжній інцидент, то, за необхідності, пересилає повідомлення на Tier 2.

Фахівець, що реагує на інциденти Tier 2, – це особа, що відповідає за проведення поглиблених розслідувань інцидентів і надання рекомендацій щодо усунення наслідків інциденту або втручання.

Tier 3 Threat Hunter – це фахівці, що мають поглиблені знання про мережі, кінцеві точки, аналітику загроз і шкідливе програмне забезпечення зворотного інжинірингу. Вони є експертами у відстеженні процесів шкідливого програмного забезпечення, щоб оцінити його вплив і визначити, як його видалити. Вони беруть активну участь у пошуку нових загроз і розгортанні програмного забезпечення для їх виявлення. Мисливці за загрозами шукають кіберзагрози, які ще не були ідентифіковані, але присутні в мережі.

Менеджер SOC – це особа, яка відповідає за ресурси SOC і виступає в ролі контактної особи з великою компанією або клієнтом (Basta et al., 2024).



Всі з перелічених вище ролей разом утворюють повноцінний моніторинг і підтримку 24/7, ручну автоматизацію. Проте в кожного кваліфікованого фахівця є обов'язки, які він виконує кожен день, і процедури, які є невід'ємною частиною процесу в SOC-команді (Vielberth et al., 2020).

Типовий день аналітика з кібербезпеки починається з перевірки черг оповіщень про загрози. Для внесення оповіщень до списку, який аналітик має дослідити, зазвичай використовують систему тікетів. Оскільки програмне забезпечення, яке генерує сповіщення, може спричиняти хибні тривоги, роль аналітика з кібербезпеки може містити підтвердження того, що тривога відображає справжній інцидент безпеки. Коли інцидент підтверджено, його можна перенаправити слідчим або іншим співробітникам служби безпеки для вжиття заходів. Якщо ні, то повідомлення може бути проігнороване як хибна тривога.

Якщо аналітик із кібербезпеки не може опрацювати повідомлення, воно буде перенаправлене до спеціаліста з реагування на інциденти рівня 2 для подальшого розгляду та виправлення. Якщо спеціаліст із реагування на інциденти не може розв'язати проблему, повідомлення переадресовують співробітникам рівня 3, які мають значні знання та досвід боротьби із загрозами.

Саме в щоденних процесах аналітика, йому на допомогу приходять сучасні технології SOC, які значно підвищують ефективність усіх етапів роботи (Akhtar, & Ali, 2021). Такі рішення, як SIEM та SOAR, не лише автоматизують рутинні завдання, а й забезпечують комплексний підхід до виявлення, аналізу та нейтралізації кіберзагроз. Розглянемо докладніше, які технологічні рішення нині формують основу сучасних центрів операційної безпеки.

SIEM розшифровує дані, отримані від брандмауерів, мережевого обладнання, систем виявлення вторгнень та інших пристроїв (Collins, 2025).

SIEM і SOAR (оркестрування, автоматизація та реагування на загрози безпеки) часто поєднуються, оскільки їхні можливості доповнюють одна одну.

Обидві технології використовуються великими командами з операцій безпеки (SecOps) для покращення SOC. Подібно до того, як SIEM-системи агрегують, порівнюють та інтерпретують попередження, платформи SOAR виконують те саме. З іншого боку, технологія SOAR робить ще один крок уперед, поєднуючи розвідку загроз і автоматизацію робочих процесів розслідування інцидентів і реагування на них на основі сценаріїв, створених командою безпеки (Vielberth et al., 2020).

Платформи безпеки SOAR:

- Збирають дані про тривоги з кожного компонента системи.
 - Надають інструменти, які дозволяють досліджувати, оцінювати та розслідувати інциденти.
 - Наголошують на інтеграції як засобі автоматизації складних робочих процесів реагування на інциденти, що забезпечує швидше реагування, та адаптивних стратегій захисту.
 - Містять заздалегідь визначені сценарії, які забезпечують автоматичне реагування на конкретні загрози.
- Плейлисти можуть бути ініційовані автоматично на основі заздалегідь визначених правил або можуть бути запущені персоналом служби безпеки.

SOAR зосереджується на інструментах автоматизації та інтеграції процесів SOC, автоматизує багато ручних процедур, таких як оповіщення про загрозу безпеці розслідування, вимагаючи участі людини, лише коли це необхідно. Це звільняє людей, які працюють у кібербезпеці, щоб зосередитися на нагальніших питаннях (Rahman, 2024).

SOAR-платформи йдуть на крок попереду, трансформуючи традиційні процеси SOC. Щоб повноцінно оцінити потенціал SOAR, важливо розібратися в його архітектурі та принципах роботи.

Іншими словами, SOAR – це категорія рішень, які спрямовані на вдосконалення шляхом інтеграції, автоматизації та уможливлення оркестрування численних інструментів і процесів безпеки. Платформи SOAR зазвичай складаються з трьох основних компонентів: координації, контролю та реагування – трьох фундаментальних методів управління. Водночас, оркестрування розуміється як взаємодія і співпраця різних рішень і додатків для забезпечення взаємної безпеки. Автоматизація в цьому сенсі передбачає використання сторонніх продуктів, які можуть впоратися із цими основними завданнями самостійно та набагато швидше без залучення команд безпеки, тим самим полегшуючи їхнє навантаження і скорочуючи час реагування (TTR-time to response). Вона також охоплює заходи, які вживають у відповідь на інциденти безпеки, які частково складаються з ідентифікації, аналізу, забруднення, видалення загрози та відновлення повністю нормального функціонала хоста, сервера тощо (BlueVoyant, 2025).

Отже, впровадження рішень SOAR дає багато переваг. Перша перевага пов'язана з підвищенням продуктивності, оскільки закупівля вхідних матеріалів у великих кількостях означає, що менше матеріалів буде витрачено на одне й те саме. Тобто покупка ліцензії для використання SOAR-систем тут повністю себе виправдовує. Таким чином, платформи SOAR значною мірою звільняють від ручної праці й оптимізують роботу кібербезпеки, автоматизуючи повторювані дії та належно контролюючи процеси. Це приводить до швидшого реагування на інциденти та кращого контролю загроз.

Ще однією перевагою є покращена видимість та обізнаність про ситуацію за допомогою рішень SOAR (Manda, 2021). Завдяки добре обробленим даним із різних джерел організації можуть використовувати SOAR для виявлення й ефективної протидії загрозам. Комплексний підхід до управління безпекою є життєво важливим для виявлення і запобігання багатогранним загрозам, які можуть виникати на різних рівнях організації.

Застосування рішень SOAR допомагає також покращити документування інцидентів безпеки та подальше звітування у разі невідповідності вимогам стандарту. Дуже багато компаній нині все більше замислюються над тим, щоб відповідати вимогам загальновідомим стандартам. Це підвищує конкурентоздатність на ринку і довіру як до компанії у сфері кібербезпеки. Контроль, який характеризує роботу більшості SOAR-платформ, гарантує документування всіх дій, вжитих у кожній точці інциденту, що дозволяє легко продемонструвати відповідність вимогам.

У такий спосіб можна забезпечити процедури аудиту на відповідність нормативним вимогам, а також у разі виникнення інциденту і для підвищення безпеки процесів. Можливості, які з'являються в впровадженні рішень SOAR, також включають масштабованість і гнучкість, що дуже важливо, особливо для великих організацій, що постійно зростають. Враховуючи постійні зміни та збільшення складності загроз безпеці, платформи SOAR можуть

рости разом із потребами організації в безпеці. Це допомагає організаціям впроваджувати надійні заходи для захисту від загроз, що постійно змінюються.

Очевидно, що рішення SOAR є життєво важливим інструментом дотримання вимог, оскільки вони детально описують можливості для покращення безпеки операцій, зміцнюють здатність організації стримувати або запобігати інцидентам, а також забезпечують прозорість загальної ситуації з безпекою. Ці переваги допомагають організаціям відповідати вимогам і залишатися в безпеці, а також забезпечують глибоке і всебічне покращення стану безпеки організації. Використовуючи рішення SOAR, будь-яка організація може гарантувати практичніший підхід до запобігання й усунення загроз безпеці, який захистить конкретні дані та забезпечить дотримання законодавства.

Сучасні кіберзагрози вимагають не лише проактивного виявлення, але й миттєвого реагування (Sironi et al., 2010). Далі розглянемо реальні кейси й імітаційні сценарії, які демонструють, як SOAR-системи допомагають SOC ефективно протистояти атакам – від фішингу до складних експлойтів. На прикладах із різних галузей (від роздрібної торгівлі до фінансового сектору) подивимось, як інтеграція оркестрації та автоматизації прискорює усунення загроз і покращує відповідність міжнародним стандартам безпеки, таким як PCI DSS.

А. Розпізнавання й усунення загроз у реальному часі (Hafa, 2025). Ще одна зафіксована атака – фішингова, в якій постраждала компанія роздрібною торгівлі; метою злоумисників було отримати облікові дані для входу в систему. В результаті, рішення SOAR змогло зупинити розсилку листів в режимі реального часу за допомогою сайту, який був підключений до системи захисту електронної пошти та продуктів розвідки загроз компанії. Згідно з аналізом операцій безпеки платформи SOAR і вимог до обізнаності, робочий процес ініціюється без затримок, щоб установити небезпечні повідомлення для ізоляції, повідомити відділ IT-безпеки, а потім заблокувати домен відправника. Крім того, після цієї кібератаки компанія була змушена ініціювати загальнокорпоративний антифішинговий тренінг, який охопив увесь персонал, щоб уникнути подібних кібератак у майбутньому. Крім зручного реагування на спробу фішингу та зупинки загрози в режимі реального часу допомагає покращити безпеку організації, не лише розв'язавши проблеми, виявлені під час експерименту.

Б. Сценарій моделювання: Clinical Experiences in ASERT (Hafa, 2025). Payment Card Industry Data Security Standard (PCI DSS) – стандарт безпеки даних індустрії платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток, заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discover.

ASERT – це елітна група інженерів і дослідників NETSCOUT, що спеціалізується на інформаційній безпеці.

Наприклад, у цій роботі слід застосувати моделювання під час упровадження SOAR у середовищі PCI DSS, де середня фірма, що займається електронною комерцією, впроваджує платформу SOAR у свою систему безпеки бізнесу. Основним напрямом діяльності фірми є впровадження стандартів PCI DSS, де важливим є встановлення моніторингу в режимі реального часу та реагування на інциденти. Платформу SOAR створено для інтеграції із SIEM, брандмауерами, IDS і системами управління вразливостями. У другому сценарії під час симуляції тестер проникнення атакує компанію, імітуючи вразливість у вебдодатку. У випадку, коли платформа SOAR виявляє аномалію, як тільки вона інтегрована із системами SIEM та IDS, вона автоматично ініціює низку дій, таких як блокування IP-адреси злоумисника, створення детального звіту про подію на сайті та надсилання тривожного повідомлення співробітникам служби безпеки на електронну пошту та мобільні номери.

Крім того, на основі виникнення CVE, яка була використана, SOAR запускає попередній сценарій, який застосовує CVE до всіх систем, щоб гарантувати, що інші не можуть бути використані подібно протягом наступних днів або тижнів. Для взаємодії з клієнтом застосовують весь процес, який був виконаний через платформу SOAR, що в подальшому може допомогти відстежувати нові виявлені інциденти безпеки, пов'язані з регулюванням PCI DSS, реагувати на них і документувати подальші дії. Оскільки рішення SOAR покращують функцію дотримання вимог PCI DSS завдяки автоматизації та оркеструванню діяльності учасників команди реагування на інциденти, вони показують, як використання платформ SOAR може привести до скорочення часу реагування; вони також допомагають у точному та належному реагуванні на інциденти безпеки і навіть слугують цінним документом для досягнення відповідності вимогам.

Розглянуті симуляції та реальні кейси наочно демонструють, як SOAR-системи трансформують реагування на кіберзагрози. Однак їхній потенціал виходить далеко за межі окремих інцидентів. У повсякденній практиці SOC платформи SOAR довели свою ефективність у розв'язанні багатьох типових завдань кібербезпеки.

1. Виявлення фішингу та реагування на нього (рис. 2).



Рис. 2. Робота SOAR при фішингу



Фішингові електронні листи є найпоширенішими, легко здійсненими атаками на безпеку (Manda, 2021; Vielberth et al., 2020). Протидія фішингу ускладнюється такими причинами:

- Велика кількість інцидентів: SOC може мати справу із сотнями або тисячами сповіщень під час загрози безпеці. Це призводить до втоми від алертів, й аналітики можуть пропустити життєво важливі індикатори поведінки загрози.
- Атаки з різних джерел: розслідування фішингу вимагає використання кількох платформ безпеки.
- Ручні операції: ручний аналіз фішингових атак вимагає годин праці.

SOAR допомагає ідентифікувати фішингові атаки за допомогою таких кроків:

Автоматичне сортування та визначення пріоритетів: системи SOAR автоматично сортують фішингові сповіщення, сортуючи потенційні загрози за ступенем серйозності, зменшуючи ручне навантаження на команди SOC.

Вилучення й аналіз показників: інструменти SOAR витягують ключові індикатори компрометації (KIC), такі як підозрілі URL-адреси, вкладення або заголовки електронних листів, і звіряють їх із відомими базами даних загроз.

Аналіз хибнопозитивних спрацьовувань: використовуючи машинне навчання та попередньо визначені правила, SOAR мінімізує помилкові спрацьовування, ідентифікуючи легітимні електронні листи, які можуть викликати фішингові сповіщення, підвищуючи точність виявлення.

2. Виявлення підозрілих входів користувачів за IP-адресами (рис. 3).



Рис. 3. Робота SOAR у разі виявлення підозрілого логіна

Проблема: підозрілі входи користувачів важко ідентифікувати з таких причин:

- Поведінку користувача важко проаналізувати;
- Компанії мають багато джерел географічного розташування та хмарних користувачів для відстеження;
- Моніторинг підозрілих входів здійснюється вручну та повторюється.

SOAR допомагає виявляти підозрілі входи користувачів за допомогою таких кроків:

Ідентифікувати поведінкові аномалії: SOAR збирає дані для входу із зовнішніх інструментів (напр., SIEM або систем автентифікації), щоб виявити незвичайні аномалії входу.

Збагатити інформацію про користувача: SOAR отримує детальну інформацію про обліковий запис користувача (напр., минулу історію входів, роль, дозволи), щоб допомогти оцінити, чи є поведінка користувача легітимною.

Збагатити IP-розвідки: SOAR порівнює IP-адреси, пов'язані зі спробою входу, з базами даних розвідки загроз, щоб перевірити їх на наявність відомих зловмисних IP-адрес.

Визначити статус загрози: на основі поведінки користувача та даних IP-розвідки SOAR автоматично вирішує, чи є спроба входу зловмисною або безпечною.

Автоматична відповідь – закрити або діяти:

- немає загрози: якщо не виявлено зловмисної активності, SOAR може автоматично закрити інциденти безпеки;
- виявлена загроза: якщо зловмисну активність підтверджено, SOAR виконує автоматичні дії, такі як блокування зловмисної IP-адреси.

3. Відстеження терміну дії SSL-сертифіката (рис. 4).



Рис. 4. Робота SOAR у разі ескалювання або закриття випадку з SSL-сертифікатом



Проблема: коли користувач намагається отримати доступ до сайту з протермінованим сертифікатом безпеки, сучасні веббраузери відображають попереджувальні повідомлення (D3Security. SOC automation examples, 2025). Це може підірвати довіру користувачів і відбити бажання відвідувачів повертатися на сайт, що потенційно може призвести до втрати трафіка і довіри до організації.

SOAR допомагає відстежувати термін дії SSL-сертифікатів:

Перевірка статусу сертифіката: SOAR безперервно відстежує SSL-сертифікати завдяки інтеграції з інструментами управління сертифікатами для перевірки їхнього статусу закінчення терміну дії.

Інформування користувача: коли термін дії сертифіката наближається до завершення, SOAR автоматично надсилає сповіщення відповідним користувачам, попереджаючи їх про наближення дати закінчення терміну дії.

Якщо термін дії сертифіката не закінчився: SOAR повторно перевіряє статус і автоматично закриває інцидент, якщо сертифікат усе ще дійсний, сповіщення буде відхилено.

Якщо термін дії закінчився: якщо термін дії сертифіката закінчився, SOAR ескалує інцидент, надсилаючи сповіщення користувачеві й іншим відповідним зацікавленим сторонам в організації.

Ескалація та комунікація: SOAR автоматично надсилає користувачеві докладні електронні листи та залучає інших важливих членів команди, забезпечуючи швидку обізнаність і дії.

Дві ключові технології, SIEM і SOAR, допомагають покращити безпеку, але мають різні переваги й обмеження.

У табл. 1 порівнюються основні критерії ефективності SIEM і SOAR: від виявлення загроз до автоматизації процесів. Це допоможе зрозуміти, яка система краще підходить для конкретних потреб організації.

Таблиця 1

Переваги використання SIEM- і SOAR-систем

Критерій	SIEM	SOAR
Виявлення загроз	Покращує виявлення складних загроз завдяки кореляції подій із різних джерел, виявляє шаблони атак	Покращує виявлення через інтеграцію з інструментами безпеки та каналами розвідки, забезпечує повний аналіз загроз
Реагування на інциденти	Надає сповіщення в реальному часі й автоматизовані дії, але основне навантаження лежить на аналітиках	Автоматизує аналіз, локалізацію та ліквідацію загроз, значно прискорює реагування
Швидкість виявлення (MTTD)	Допомагає зменшити час виявлення, але залежить від налаштувань і ручного аналізу	Значно скорочує MTTR завдяки автоматизації та інтегрованим сценаріям
Швидкість реагування (MTTR)	Частково автоматизує процеси, але MTTR залишається високим через необхідність ручного втручання	Різко знижує MTTR завдяки автоматизованим робочим процесам (блокування IP-адрес, ізоляція загроз тощо)
Видимість загроз	Забезпечує централізований аналіз даних, але може бути обмеженим у комплексному розумінні загроз	Надає глибшу видимість завдяки інтеграції з різними системами та розвідкою загроз
Автоматизація	Автоматизує збір логів, аналіз і звітність, але не замінює ручну роботу	Автоматизує більшість рутинних завдань (розслідування, реагування, документування)
Ефективність SOC	Підвищує ефективність завдяки централізації даних, але не усуває втому від оповіщень	Оптимізує роботу SOC, звільняючи аналітиків для стратегічних завдань (полювання на загрози, управління вразливостями)
Складність впровадження	Відносно простий у налаштуванні, але вимагає постійного оновлення правил кореляції	Вимагає глибокого планування, чітких сценаріїв і кваліфікованого персоналу
Підтримка малих організацій	Підходить для малих і середніх компаній, оскільки може масштабуватися	Може бути надмірним для малих команд через складність і вартість

Проаналізувавши цю таблицю, можемо зазначити, що SIEM є ефективним інструментом для моніторингу, виявлення загроз і часткової автоматизації, але його можливості обмежені в плані швидкого реагування.

SOAR значно перевершує SIEM в автоматизації реагування, скороченні MTTR/MTTD і покращенні продуктивності SOC, але вимагає більших ресурсів для впровадження.

Оптимальний підхід, який ми запропонували б для компаній або організацій:

- SIEM – база для моніторингу й аналізу.
- SOAR – надбудова для автоматизації та прискорення реагування.
- Інтеграція SIEM + SOAR дає максимальний ефект, поєднуючи сильні сторони обох технологій (рис. 5).

Джерела даних (Data Sources):

- Промислові системи: SCADA, PLC, датчики, DCG-системи (критична інфраструктура).
- IT-інфраструктура: мережеві пристрої, сервери, бази даних, додатки, хмарні сервіси.
- Інструменти безпеки: фаєрволи, системи виявлення вторгнень (IDS).

Оброблення даних:

- Дані з усіх джерел надходять до SEM (Security Event Management) для аналізу та кореляції подій.
- SOAR автоматизує реагування на загрози.

Функціональні модулі:

- Моніторинг відповідності (Compliance Monitoring & Reporting): перевірка на відповідність стандартам (GDPR, ISO 27001 тощо).
- Розвідка загроз (Threat Intelligence): аналіз IOC (індикаторів компрометації), пошук нових загроз.



- Реагування на інциденти (Incident Response): автоматизовані сценарії (блокування IP, відключення акаунтів тощо).
- Роль аналітика (Security Analyst):
- Отримує структуровані алерти, досліджує інциденти, приймає рішення на основі даних від SOAR/SIEM.

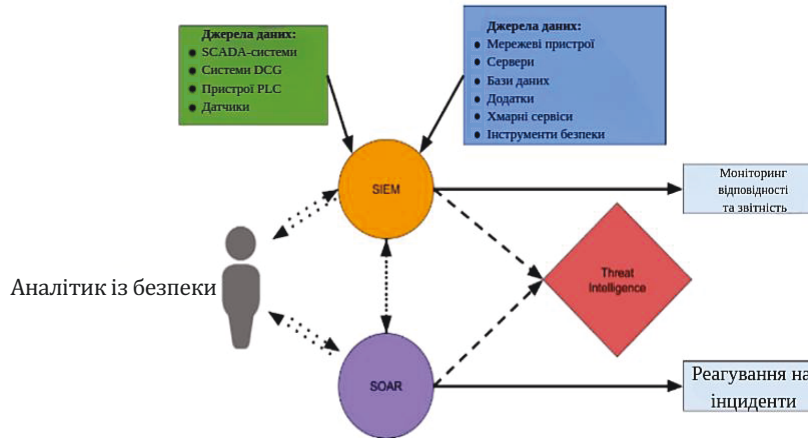


Рис. 5. Взаємодія між SOAR- і SIEM-системами

Система автоматично обробляє тисячі сповіщень про можливі загрози, фільтрує їх і залишає аналітикам лише найважливіші випадки. Працює як помічник, що бере на себе всі нудні завдання. Вона збирає інформацію з усіх кутків мережі – від офісних комп'ютерів до промислових систем і хмарних сервісів. Тепер не треба перемикатися між десятком різних програм. Коли знаходить реальну загрозу, система може миттєво її зупинити – наприклад, заблокувати зловмисника або вимкнути зламаний обліковий запис, навіть якщо це сталося серед ночі. Сама готує всі необхідні звіти для перевірок, що дуже зручно, коли потрібно довести, що все відповідає стандартам безпеки. Система постійно оновлює свої знання про нові віруси та методи хакерів, тому із часом стає тільки розумнішою. Чи то звичайні офісні комп'ютери, чи то складні промислові системи – система SOAR впорається з моніторингом усього. Головний плюс – вона дає можливість невеликій команді фахівців ефективно контролювати велику мережу, швидше знаходити проблеми і вчасно на них реагувати. Це як потужний підсилювач для кібербезпеки.

Хоча система SOAR є дуже повною і функціональною платформою, важливо зазначити, що координація дуже важлива, оскільки SOAR не є повністю автоматизованим сервісом. SOAR потребує від команди кібербезпеки чіткого сценарію використання, міцної основи, навичок і вимог до операційної моделі, а також постійного технічного обслуговування для належної роботи. Суттєво також знати, які очікування команди безпеки покладають на платформу, і знайти відповідний варіант використання для того, що вони намагаються вирішити.

Важливо також зазначити, що для команд безпеки, які працюють у невеликих організаціях і повинні виконувати лише базові процедури і процеси, платформа SOAR може бути не найкращим варіантом, оскільки вона не буде відповідати їхнім потребам.

Дискусія і висновки

Сучасний стан кібербезпеки з його стрімким зростанням кількості та складності загроз робить SOAR-системи незамінним інструментом для центрів операційної безпеки. Ці системи не лише автоматизують рутинні процеси, а й забезпечують ефективну оркестрацію різноманітних інструментів кібербезпеки, що значно прискорює реагування на інциденти та підвищує точність їх виявлення. Інтегруючись із такими системами як SIEM, EDR та Threat Intelligence платформами, SOAR уможливорює зменшення навантаження на аналітиків SOC, скорочуючи час реагування (MTTR) і мінімізуючи вплив людського фактора. Для організацій з обмеженими ресурсами ключовим аспектом успішного впровадження SOAR є поетапний підхід, який передбачає спочатку автоматизацію найкритичніших процесів, таких як класифікація інцидентів чи блокування загроз. Причому важливо враховувати наявність кваліфікованих фахівців, оскільки ефективне використання SOAR вимагає не лише налаштування відповідних playbooks, а й постійного оновлення сценаріїв реагування відповідно до нових викликів. Оцінювання ефективності SOAR-систем базується на кількох ключових показниках, серед яких найважливішими є скорочення часу реагування, зменшення кількості ручних операцій, підвищення якості аналізу за рахунок зниження кількості хибно-позитивних спрацьовувань, а також можливість масштабування системи у міру зростання кількості загроз. Важливо розуміти, що SOAR не замінює традиційні SIEM-системи, а слугує їх логічним доповненням, розширюючи функціонал завдяки автоматизації та оркестрації процесів. Для досягнення максимальної ефективності від упровадження SOAR необхідно ретельно підійти до процесу планування. Першим кроком має стати комплексний аудит інфраструктури з визначенням пріоритетних напрямів автоматизації. Вибір платформи варто здійснювати з урахуванням її гнучкості та сумісності з існуючими інструментами. Розроблення стандартних playbooks для найпоширеніших сценаріїв загроз, таких як фішинг, DDoS-атаки або malware-інфекції, дозволить швидше отримати відчутні результати. Одночасно необхідно забезпечити навчання персоналу та впровадити систему моніторингу ефективності, яка дозволяла б відстежувати ключові показники на кшталт MTTR чи кількості автоматизованих інцидентів. Оптимальними умовами для успішного функціонування SOAR є наявність інтегрованого середовища кібербезпеки, чітко визначених процесів реагування на інциденти та кваліфікованої команди, здатної підтримувати й розвивати систему. У сучасних умовах,



коли кіберзагрози постійно еволюціонують, а кількість фахівців з безпеки залишається обмеженою, SOAR-системи стають стратегічним рішенням для підвищення продуктивності й ефективності роботи SOC. Проте їх успішне використання вимагає не лише технічної готовності інфраструктури, а й організаційної зрілості команди, що дасть змогу повною мірою реалізувати потенціал цих складних, але надзвичайно корисних інструментів кібербезпеки.

Внесок авторів: Іван Опірський – концептуалізація дослідження; методологія; загальне керівництво проєктом; аналіз сучасного стану кібербезпеки та ролі SOC; формулювання мети та завдань дослідження; розроблення теоретичної бази дослідження SOAR-технологій; огляд літератури й аналіз останніх досліджень у сфері автоматизації кібербезпеки; формулювання загальних висновків і перспектив подальших досліджень. Соломія Яворівська – аналіз методів інтеграції SOAR з існуючими системами безпеки; порівняльний аналіз ефективності автоматизованих і ручних процесів реагування на інциденти; дослідження критеріїв успішності впровадження SOAR для організацій з обмеженими ресурсами; розроблення практичних рекомендацій щодо поетапного впровадження платформ оркестрації; створення схем взаємодії між SOAR- і SIEM-системами; візуалізація процесів автоматизації; підготовка діаграм і рисунків; розроблення рекомендацій з оптимізації робочих процесів SOC із використанням сучасних SOAR-платформ.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Akhtar, S., & Ali, S. (2021). *Machine learning in SOC operations: Transforming incident detection and response*. <https://doi.org/10.13140/RG.2.2.13839.29605>
- Basta A., Basta N., Waqar Anwar M., & Essar L. (2024). *Open-source security operations center (SOC): A complete guide to establishing, managing, and maintaining a modern SOC*. John Wiley & Sons.
- BlueVoyant. (2025). *SOAR security: How it works, use cases, and key features*. Retrieved December 4, 2025, from <https://www.bluevoyant.com/knowledge-center/soar-security-how-it-works-use-cases-and-key-features>
- Brewer, R. (2019). Could SOAR save skills-short SOC's? *Computer Fraud & Security*, 2019(4), 8–11. [https://doi.org/10.1016/S1361-3723\(19\)30106-X](https://doi.org/10.1016/S1361-3723(19)30106-X)
- Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2023). *Testing SOAR tools in use*. *Computers & Security*, 129, 103201. <https://doi.org/10.1016/j.cose.2023.103201>
- Chatterjee, S. (2020). *Using SIEM and SOAR for real-time cybersecurity operations in oil and gas*. *IJIRCT*. <https://doi.org/10.5281/ZENODO.14598693>
- Collins, Z. (2025, June 3). *Top 7 SOAR tools (as of 2025)*. OnPage. <https://www.onpage.com/top-7-soar-tools-as-of-2025/>
- D3Security. *SOC automation examples*. <https://d3security.com/blog/soc-automation-examples/>
- Hafa, A. (2025). *SOAR use cases*. AI Multiple. <https://aimultiple.com/soar-use-cases>
- Manda, J. K. (2021). Cybersecurity automation in telecom: Implementing automation tools and technologies to enhance cybersecurity incident response and threat detection in telecom operations. *Advances in Computer Sciences*, 4(1).
- Noshi, A., & Blaser, F. (2024). *Integrating artificial intelligence and machine learning for advanced cyber security in SOC operations*. <https://doi.org/10.13140/RG.2.2.21176.05121>
- Rahman, A. (2024). *Applications of artificial intelligence for protecting software supply chains (SSCs) in the defense industrial base (DIB)*. CSIAc. https://csiac.dtic.mil/wp-content/uploads/2024/02/SOAR_CSIAC_Applications-of-Artificial-Intelligence-AI-for-Protecting-Software-Supply-Chains-SSCs-in-the-Defense-Industrial-Base-DIB_032724-contract.pdf
- Seeton. (2025). *Автоматизація реагування на інциденти (рішення SOAR)*. <https://www.seeton.pro/cybersecurity/soar/>
- Sharma, A., & Spunda, R. (2025). *SOC optimization through AI-powered automation and blockchain integration*. <https://doi.org/10.13140/RG.2.2.27709.99049>
- Sironi, F., Triverio, M., Hoffmann, H., Maggio, M., & Santambrogio, M. (2010). Self-aware adaptation in FPGA-based systems. In *Proceedings of the 2010 International Conference on Field Programmable Logic and Applications (FPL)* (pp. 187–192). <https://doi.org/10.1109/FPL.2010.43>
- Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227787. <https://doi.org/10.1109/ACCESS.2020.3045514>
- Woods, D. D., Johannesen, L. J., Cook, R. I., & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight*. The Ohio State University.

References

- Akhtar, S., & Ali, S. (2021). *Machine learning in SOC operations: Transforming incident detection and response*. <https://doi.org/10.13140/RG.2.2.13839.29605>
- Basta A., Basta N., Waqar Anwar M., & Essar L. (2024). *Open-source security operations center (SOC): A complete guide to establishing, managing, and maintaining a modern SOC*. John Wiley & Sons.
- BlueVoyant. (2025). *SOAR security: How it works, use cases, and key features*. Retrieved December 4, 2025, from <https://www.bluevoyant.com/knowledge-center/soar-security-how-it-works-use-cases-and-key-features>
- Brewer, R. (2019). Could SOAR save skills-short SOC's? *Computer Fraud & Security*, 2019(4), 8–11. [https://doi.org/10.1016/S1361-3723\(19\)30106-X](https://doi.org/10.1016/S1361-3723(19)30106-X)
- Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2023). *Testing SOAR tools in use*. *Computers & Security*, 129, 103201. <https://doi.org/10.1016/j.cose.2023.103201>
- Chatterjee, S. (2020). *Using SIEM and SOAR for real-time cybersecurity operations in oil and gas*. *IJIRCT*. <https://doi.org/10.5281/ZENODO.14598693>
- Collins, Z. (2025, June 3). *Top 7 SOAR tools (as of 2025)*. OnPage. <https://www.onpage.com/top-7-soar-tools-as-of-2025/>
- D3Security. *SOC automation examples*. <https://d3security.com/blog/soc-automation-examples/>
- Hafa, A. (2025). *SOAR use cases*. AI Multiple. <https://aimultiple.com/soar-use-cases>
- Manda, J. K. (2021). Cybersecurity automation in telecom: Implementing automation tools and technologies to enhance cybersecurity incident response and threat detection in telecom operations. *Advances in Computer Sciences*, 4(1).
- Noshi, A., & Blaser, F. (2024). *Integrating artificial intelligence and machine learning for advanced cyber security in SOC operations*. <https://doi.org/10.13140/RG.2.2.21176.05121>
- Rahman, A. (2024). *Applications of artificial intelligence for protecting software supply chains (SSCs) in the defense industrial base (DIB)*. CSIAc. https://csiac.dtic.mil/wp-content/uploads/2024/02/SOAR_CSIAC_Applications-of-Artificial-Intelligence-AI-for-Protecting-Software-Supply-Chains-SSCs-in-the-Defense-Industrial-Base-DIB_032724-contract.pdf
- Seeton. *Автоматизація реагування на інциденти (рішення SOAR)*. <https://www.seeton.pro/cybersecurity/soar/>
- Sharma, A., & Spunda, R. (2025). *SOC optimization through AI-powered automation and blockchain integration*. <https://doi.org/10.13140/RG.2.2.27709.99049>
- Sironi, F., Triverio, M., Hoffmann, H., Maggio, M., & Santambrogio, M. (2010). Self-aware adaptation in FPGA-based systems. In *Proceedings of the 2010 International Conference on Field Programmable Logic and Applications (FPL)* (pp. 187–192). <https://doi.org/10.1109/FPL.2010.43>
- Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227787. <https://doi.org/10.1109/ACCESS.2020.3045514>
- Woods, D. D., Johannesen, L. J., Cook, R. I., & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight*. The Ohio State University.

Отримано редакцією журналу / Received: 04.11.25

Прорецензовано / Revised: 08.11.25

Схвалено до друку / Accepted: 21.12.25



Ivan OPIRSKYI, DSc (Engin.), Prof.
ORCID ID: 0000-0002-8461-8996
e-mail: ivan.r.opirskyi@lpnu.ua
Lviv Polytechnic National University, Lviv, Ukraine

Solomiia YAVORIVSKA, Student
ORCID ID: 0009-0002-0018-6231
e-mail: solomiia.yavorivska.kb.2023@lpnu.ua
Lviv Polytechnic National University, Lviv, Ukraine

RESEARCH ON THE FEATURES OF USING SOAR AS A PRIMARY TOOL FOR ACCELERATING INCIDENT RESPONSE

Background. The intensive development of cyber threats and their increasing complexity in the modern digital environment create critical challenges for Security Operations Centers (SOC), which require new approaches to automation and orchestration of cybersecurity processes. One of the key problems of modern SOC is the need to process vast volumes of threat information, rapidly respond to incidents, and coordinate actions between different security systems with limited human resources. In the context of a shortage of qualified cybersecurity professionals, SOAR (Security Orchestration, Automation, and Response) platforms, which can automate routine processes without compromising analysis quality, become particularly relevant. The application of integrated orchestration mechanisms, specifically automation of phishing response, coordination between SIEM systems, and incident management, form the foundation of modern approaches to effective SOC functioning.

Methods. The study conducted a systematic analysis of contemporary methods for implementing SOAR systems in security operations centers, particularly in the context of integration with existing SIEM platforms. Comparative analysis methods, threat scenario modeling, practical testing of automated workflows, and evaluation of the effectiveness of various implementation strategies were employed. Special attention was given to analyzing key performance indicators, such as reducing mean time to detection (MTTD) and mean time to response (MTTR), automating incident classification processes, and integrating with threat intelligence sources. For each approach, implementation complexity, personnel qualification requirements, economic efficiency, and compatibility with existing SOC architecture were assessed.

Results. The analysis revealed that the most effective approach to SOC optimization is the combination of SOAR platforms with traditional SIEM systems in the form of a complementary ecosystem. For instance, using automated playbooks for phishing response significantly reduces reaction time from hours to minutes, while integration with threat intelligence systems prevents missing critical indicators of compromise. It was demonstrated that combining automation of routine tasks with human control of strategic decisions significantly enhances SOC analyst productivity and accuracy in detecting genuine threats. Simultaneously, SOAR implementation requires careful planning and a phased approach, especially for organizations with limited resources. Optimal implementation strategies were identified based on organization size, cybersecurity process maturity level, and availability of qualified personnel.

Conclusions. Optimizing security operations centers through SOAR technology implementation requires a systematic and comprehensive approach that considers both technical and organizational aspects. Combining automation with human expertise enables achieving high levels of efficiency without losing control over critical security processes. The research results can be utilized for building integrated cybersecurity systems considering the limited resources of small and medium organizations. Beyond technical-economic aspects, the importance of phased implementation, personnel training, and continuous improvement of automated scenarios in accordance with cyber threat evolution is emphasized. Systematic implementation of SOAR approaches will ensure enhanced SOC efficiency even under conditions of increasing quantity and complexity of cyber incidents.

Keywords: SOAR, SOC, cybersecurity, incident response automation, SIEM, threat orchestration, MTTD, MTTR, security tools integration, incident documentation, threat analytics, SOC optimization.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript or in the publication of the results.