УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.16

Я. А. МАРТИНЕНКО
магістрант кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0005-2958-0592

О. В. СЄВЄРІНОВ
кандидат технічних наук, доцент,
професор кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-6327-6405

А. М. ЄВГЕНЬЄВ
старший викладач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-4365-5675

М. С. СКИБЕНКО
старший викладач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0002-4838-9329

ДОСЛІДЖЕННЯ SOAR-ПЛАТФОРМ ТА ОБҐРУНТУВАННЯ ВИБОРУ SPLUNK PHANTOM

У статті досліджено особливості застосування SOAR-платформ у контексті підвищення ефективності центрів моніторингу безпеки (SOC) за умов зростання складності корпоративних інфраструктур, збільшення кількості кіберінцидентів та розширення використання хмарних сервісів. Проаналізовано ключові проблеми, з якими стикаються аналітики SOC, зокрема великий обсяг подій, високий рівень хибнопозитивних сповіщень та обмеженість традиційних систем моніторингу, що не забезпечують автоматизованого реагування. Розглянуто архітектуру сучасних SOAR-платформ, яка охоплює інтеграційний, оркестраційно-аналітичний та операційний шари, а також принципи їх взаємодії з SIEM, EDR, IDS/IPS, системами керування вразливостями й платформами threat intelligence.

У роботі досліджено моделі автоматизації та оркестрації інцидентів, зокрема rule-based, state-based та context-aware підходи, які формують основу сучасних playbooks та забезпечують зниження навантаження на аналітиків, підвищення швидкості реагування та стандартизацію процесів. Окрему увагу приділено метрикам оцінювання ефективності SOAR-рішень, таким як MTTD, MTTR, Automation Coverage та False Positive Ratio, а також методам тестування масштабованості та інтеграційної надійності.

Представлено порівняльний аналіз провідних рішень: Splunk Phantom, Cortex XSOAR, IBM Resilient та Chronicle SOAR, із визначенням їх ключових переваг і обмежень. Показано, що Splunk Phantom вирізняється збалансованою архітектурою, гнучкою моделлю containers–artifacts, широкими можливостями інтеграції, підтримкою Python-скриптів та здатністю до побудови складних сценаріїв реагування. Отримані результати дозволяють визначити місце SOAR-платформ як ключового елемента сучасної інфраструктури кібербезпеки та підкреслити їхню роль у створенні відтворюваних, контрольованих і стандартизованих процесів реагування.

Ключові слова: *SOAR, SOC, автоматизація реагування, оркестрація інцидентів, Splunk Phantom, playbooks, кіберінциденти.*

YA. A. MARTYNENKO
Master's Student at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0005-2958-0592

O. V. SIEVIERINOV
Candidate of Technical Sciences, Associate Professor,
Professor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-6327-6405

A. M. YEVHENIEV
Senior Instructor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0003-4365-5675

M. S. SKYBENKO
Senior Instructor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0002-4838-9329

RESEARCH ON SOAR PLATFORMS AND JUSTIFICATION FOR CHOOSING SPLUNK PHANTOM

The article examines the features of SOAR platforms in the context of improving the efficiency of security operations centers (SOCs) amid growing complexity of corporate infrastructures, increasing number of cyber incidents, and expanding use of cloud services. It analyzes the key problems faced by SOC analysts, including the large volume of events, the high level of false positives, and the limitations of traditional monitoring systems that do not provide automated response. The architecture of modern SOAR platforms is considered, covering the integration, orchestration and analytics, and operational layers, as well as the principles of their interaction with SIEM, EDR, IDS/IPS, vulnerability management systems, and threat intelligence platforms.

The paper explores models of incident automation and orchestration, in particular rule-based, state-based, and context-aware approaches, which form the basis of modern playbooks and reduce the workload on analysts, increase response speed, and standardize processes. Special attention is paid to metrics for evaluating the effectiveness of SOAR solutions, such as MTTD, MTTR, Automation Coverage, and False Positive Ratio, as well as methods for testing scalability and integration reliability.

A comparative analysis of leading solutions: Splunk Phantom, Cortex XSOAR, IBM Resilient, and Chronicle SOAR, is presented, identifying their key advantages and limitations. It is shown that Splunk Phantom stands out with its balanced architecture, flexible containers–artifacts model, extensive integration capabilities, support for Python scripts, and ability to build complex response scenarios. The results obtained allow us to define the place of SOAR platforms as a key element of modern cybersecurity infrastructure and emphasize their role in creating reproducible, controllable, and standardized response processes.

Key words: *SOAR, SOC, response automation, incident orchestration, Splunk Phantom, playbooks, cyber incidents.*

Постановка проблеми

У сучасних умовах центри моніторингу безпеки стикаються зі стрімким збільшенням кількості подій, значна частина з яких є хибно-позитивними або повторюваними. Традиційні засоби моніторингу фокусуються на зборі та кореляції даних, але не забезпечують автоматизованих механізмів оперативного реагування, що призводить до зростання навантаження на аналітиків SOC та збільшення часу обробки інцидентів. Відсутність стандартизованих, масштабованих та відтворюваних процесів реагування ускладнює забезпечення стабільної роботи SOC і знижує ефективність протидії кіберзагрозам. Це формує необхідність у впровадженні рішень, здатних автоматизувати рутинні задачі, стандартизувати процеси та підвищити швидкість реагування.

Аналіз останніх досліджень і публікацій

У сучасній науково-практичній літературі помітно посилення інтересу до проблем автоматизації реагування на кіберінциденти, оцінювання ефективності SOAR-платформ та їхньої інтеграції в інструментальний стек SOC. У роботі, присвяченій оркестрації, автоматизації та реагуванню, робить наголос на практичному застосуванні SOAR для підвищення ключових операційних показників SOC, зокрема, скорочення середнього часу на виявлення/реагування (MTTA/MTTR) та зміцнення безпекової позиції організації [1]. Книга має прикладну спрямованість і служить практичним керівництвом для аналітиків, які впроваджують та налаштовують сценарії реагування (playbooks) у реальних середовищах.

Практичні аспекти інтеграції SIEM-рішень у робочі процеси SOC висвітлені в праці Marlette, підкреслюють важливість правильної інтеграції SOAR-рішень із системами моніторингу та аналітики, зокрема SIEM. Зазначається, що ефективність автоматизованих сценаріїв реагування залежить від коректної побудови кореляційних правил, якості початкових даних і здатності інструментів забезпечувати взаємодію між підсистемами кіберзахисту [2].

У статті [3] розглядається питання автоматизації безпеки в хмарних середовищах, фокусуючись на балансі між виявленням загроз та заходами реагування. Ця робота має безпосереднє відношення до теми SOAR, адже архітектури сучасних SOC дедалі частіше охоплюють гібридні та хмарні інфраструктури, де питання масштабованості, інтеграції і узгодженості автоматизованих дій набувають ключового значення.

Результати щодо використання SOAR-інструментів у реальних умовах надають Bridges та співавтори у своїй статті, що демонструє практичні переваги та обмеження існуючих рішень. Автори вказують на позитивний вплив SOAR на продуктивність аналітиків та швидкість виконання рутинних дій, але також підкреслюють потребу в ретельному налаштуванні, оцінці human-in-the-loop інтервенцій та перевірці сценаріїв у контрольованому середовищі перед розгортанням у продакшн [4]. Такий підхід підтверджує тезу про необхідність комбінованого тестування як формального, так і практичного.

В [5] розвивається тема гіперавтоматизації, пропонуючи підходи з використанням «agentic» штучного інтелекту для динамічного формування workflows та підтримки експертів SOC. Робота демонструє, що поєднання AI-агентів із SOAR-інструментами може підвищити адаптивність сценаріїв реагування, проте вимагає уваги до контролю, аудиту та визначення меж автоматизації, аби уникнути небажаних дій чи помилкових ескалацій у продакшн-середовищі.

Аналіз літератури свідчить, що SOAR-платформи розглядаються як ключовий елемент сучасної архітектури кіберзахисту. Дослідження підтверджують їхню здатність підвищувати ефективність SOC, оптимізувати процеси реагування, забезпечувати узгодженість дій аналітиків та зменшувати час обробки інцидентів.

Формулювання мети дослідження

Метою дослідження є аналіз можливостей SOAR-платформ у контексті підвищення ефективності роботи SOC, визначення їх архітектурних та функціональних особливостей, оцінювання моделей автоматизації реагування та порівняння провідних рішень ринку. Особлива увага приділяється виявленню переваг Splunk Phantom як інструмента, що забезпечує високий рівень автоматизації, гнучкість побудови сценаріїв реагування та масштабованість, необхідну для сучасних корпоративних середовищ.

Викладення основного матеріалу дослідження

Зростання кількості кіберінцидентів, розширення корпоративних інфраструктур, використання хмарних сервісів та віддалених робочих місць формують нові виклики для центрів моніторингу безпеки (SOC). Аналітики стикаються з великою кількістю подій, значна частина яких є хибнопозитивними або повторюваними. За даними звітів провідних компаній з кібербезпеки, SOC-фахівці щоденно отримують від 5 000 до 50 000 подій, що підлягають аналізу. У таких умовах традиційні засоби моніторингу перестають бути достатніми, оскільки їхня функціональність зосереджена на зборі та кореляції подій, але не забезпечує автоматичного реагування.

SOAR-платформи вирішують цю проблему, надаючи можливість [1]:

– автоматизувати рутинні процеси;
– зменшити залежність від людського фактору;
– структурувати обробку інцидентів за уніфікованими процесами;
– швидко залучати додаткові джерела інформації (threat intel);
– документувати реагування згідно зі стандартами (NIST, ISO 27035).

Таким чином, SOAR стає ключовим елементом сучасної архітектури SOC, посилюючи традиційні засоби моніторингу.

Архітектура та ключові компоненти SOAR-платформ

Архітектура SOAR-платформ є багатокомпонентною структурою, спрямованою на забезпечення автоматизованого, стандартизованого та масштабованого реагування на кіберінциденти в межах центрів моніторингу безпеки. Типова SOAR-система складається з трьох ключових шарів: інтеграційного, оркестраційно-аналітичного та операційного. Інтеграційний шар забезпечує підключення до зовнішніх систем безпеки, такі як SIEM, EDR, IDS/IPS, фаєрволів, систем керування вразливостями, а також платформ Threat Intelligence. Взаємодія здійснюється через REST API, webhooks або спеціалізовані конектори, що дозволяє агрегувати інформацію з різнорідних джерел у єдине середовище аналізу.

На рисунку 1 подано узагальнену архітектуру SOAR-платформи, яка демонструє основні джерела даних, інтеграційні механізми, а також логічні блоки оркестрації та адаптивного реагування [1].

Оркестраційно-аналітичний шар відповідає за обробку подій, їх кореляцію, класифікацію та побудову автоматизованих сценаріїв (playbooks). Саме в цьому компоненті реалізуються логіка умовних переходів, ескалація інцидентів, валідація даних та прийняття рішень на основі контексту.

Багато платформ додатково використовують машинне навчання або правила поведінкового аналізу для зменшення кількості хибно-позитивних сповіщень.

Операційний шар підтримує взаємодію аналітиків із системою, забезпечуючи інтерфейси для відстеження інцидентів, ухвалення рішень, документування та контролю виконання. Тут реалізовані механізми контролю доступу, аудит дій, збереження артефактів та формування звітності відповідно до стандартів NIST чи ISO 27035.

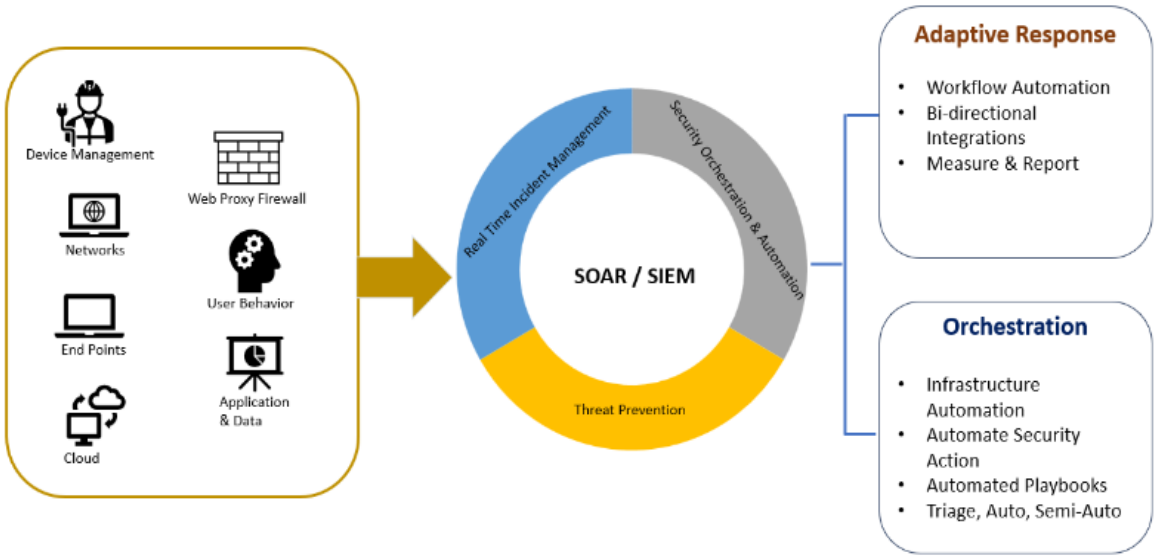

Рис. 1. Узагальнена архітектура SOAR-платформи

Подібна архітектура SOAR-платформ дозволяє не лише автоматизувати виконання рутинних завдань, а й створити узгоджене середовище реагування, де кожний інцидент проходить через стандартизований, контрольований і відтворюваний процес обробки.

Моделі автоматизації та оркестрації інцидентів

Автоматизація та оркестрація інцидентів у межах SOAR-платформ ґрунтуються на побудові формалізованих сценаріїв реагування, які забезпечують відтворюваність, швидкість та зниження навантаження на аналітиків SOC. У сучасних системах використовуються кілька моделей реалізації автоматизованих дій, серед яких найпоширенішими є rule-based, state-based та context-aware підходи.

Rule-based модель передбачає виконання фіксованих правил, що визначають логіку обробки інциденту відповідно до умов тригерів. Такий підхід є найпростішим, проте може потребувати значної кількості ручного налаштування у складних середовищах. State-based модель оперує станами інциденту, де кожен етап реагування відповідає певному вузлу workflow, а переходи між станами залежать від результатів попередніх дій. Це дозволяє реалізувати багатоетапні процеси, включаючи паралельне виконання задач та адаптацію сценарію в реальному часі. Context-aware автоматизація є найбільш гнучкою, оскільки враховує особливості інциденту, середовище виконання, попередню історію подій та поведінкові характеристики. Такий підхід дозволяє мінімізувати хибно-позитивні сповіщення, автоматично визначати пріоритетність інцидентів та оптимізувати вибір заходів реагування.

На рисунку 2 наведено повний цикл автоматизації та оркестрації інцидентів, що охоплює етапи збору подій, нормалізації, збагачення, прийняття рішень та виконання дій. Схема ілюструє взаємодію між аналітичними модулями SOAR, зовнішніми джерелами подій та системами, що забезпечують реагування.

Типові автоматизовані дії SOAR охоплюють enrichment (збагачення даних), containment (локалізація загрози), remediation (усунення наслідків), а також документування та ескалацію. Стандарти NIST Incident Response Lifecycle природно лягають у структуру playbooks, забезпечуючи відповідність кращим практикам реагування. Завдяки цим моделям SOAR-системи створюють цілісний цикл оркестрації, який дозволяє значно скоротити MTTR та підвищити ефективність SOC.

Оцінка ефективності SOAR: метрики, показники та методи тестування

Оцінювання ефективності SOAR-платформ є важливим етапом впровадження та оптимізації процесів реагування в SOC, оскільки дозволяє визначити реальний вплив автоматизації на швидкість, точність і якість обробки інцидентів. Для цього використовують комплекс метрик, що охоплюють як технічні аспекти роботи системи, так і організаційні показники взаємодії аналітиків із платформою [4-6].

До ключових метрик належать Mean Time to Detect (MTTD) та Mean Time to Respond (MTTR), які відображають середній час виявлення та реагування на інциденти. Зниження MTTR є основним показником успішності автоматизації, оскільки SOAR забезпечує швидке виконання дій, які раніше виконувалися вручну. Іншим важливим показником є Automation Coverage, що демонструє частку етапів обробки інцидентів, повністю або частково автоматизованих. Метрика False Positive Ratio дозволяє оцінити, наскільки правильно платформа фільтрує хибно-позитивні події, зменшуючи непотрібне навантаження на аналітиків.

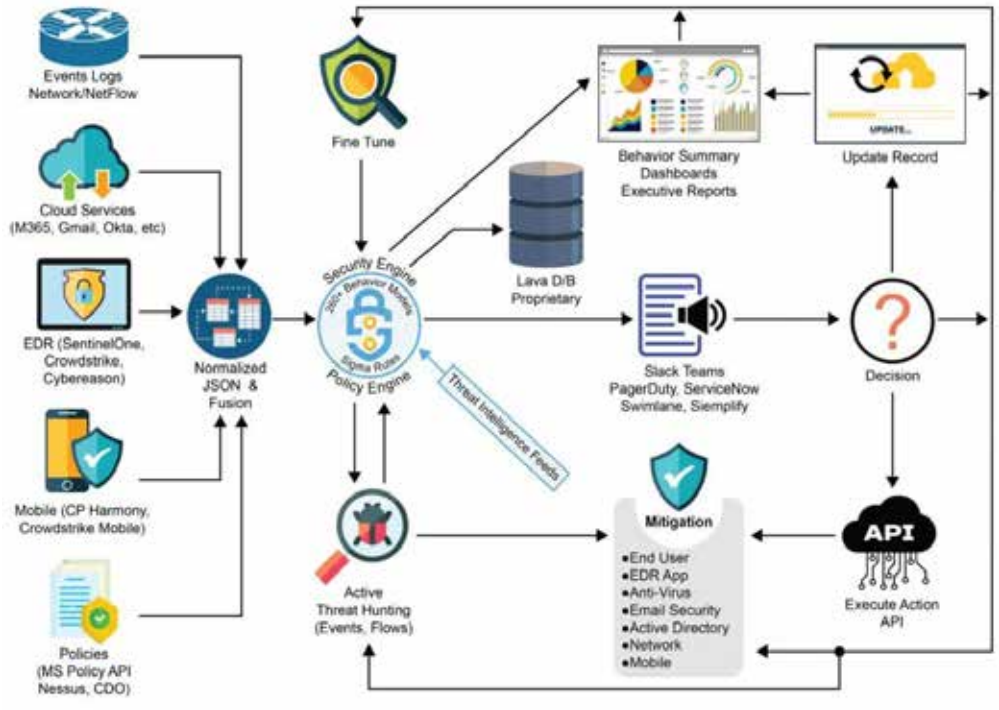

Рис. 2. Цикл автоматизації та оркестрації інцидентів у SOAR-платформі

У таблиці 1 узагальнено основні метрики та методи перевірки ефективності SOAR-рішень, що дозволяють комплексно оцінити швидкість, точність та якість автоматизованого реагування.

Методи тестування SOAR-рішень включають моделювання інцидентів, створення контрольованих сценаріїв з різними рівнями складності, а також валідацію інтеграційних дій із зовнішніми системами. Важливим є також проведення тестів на стійкість та масштабованість для оцінки можливостей системи обробляти великий обсяг подій.

Таблиця 1

Ключові метрики та методи оцінювання ефективності SOAR-платформ

Метрика / Метод	Опис	Призначення та інтерпретація
MTTD (Mean Time to Detect)	Середній час від появи інциденту до його виявлення	Показує ефективність кореляції та тригерів
MTTR (Mean Time to Respond)	Час від підтвердження інциденту до завершення реагування	Ключовий показник ефективності автоматизації; демонструє, наскільки SOAR скорочує цикл реагування
Automation Coverage	Частка кроків обробки інцидентів, що автоматизовані	Дозволяє оцінити ступінь зрілості та навантаження на аналітиків; високий рівень корелює зі зниженим MTTR
False Positive Ratio	Відношення хибно-позитивних подій до загальної кількості алертів	Дає змогу оцінити точність фільтрації й коректність інтеграцій; важливо для зменшення SOC-fatigue
Scenario-based Testing	Моделювання реальних інцидентів із різним рівнем складності	Дозволяє перевірити поведінку playbook'ів, надійність логіки та коректність автоматизованих рішень
Integration Validation	Перевірка роботи API, конекторів та зовнішніх сервісів	Виявляє проблеми зі збагаченням, containment-діями та взаємодією з інструментами безпеки
Stress & Scalability Tests	Навантажувальні тести (високий потік подій, паралельні workflow)	Дають розуміння, чи здатна платформа працювати в умовах пікового SOC-навантаження

Комплексний аналіз цих метрик дозволяє визначити, наскільки впроваджена SOAR-платформа відповідає вимогам SOC та чи забезпечує вона покращення безпекових процесів у порівнянні з традиційними методами [4-6].

Порівняльний аналіз провідних SOAR-платформ

Порівняльний аналіз сучасних SOAR-платформ є ключовим етапом вибору оптимального рішення для впровадження в інфраструктуру центру моніторингу безпеки. Ринок SOAR-технологій представлений кількома зрілими продуктами, серед яких найбільш відомими є Splunk Phantom, Palo Alto Cortex XSOAR, IBM Resilient та Google Chronicle SOAR (раніше Siemplify). Кожна з перелічених платформ має власний підхід до автоматизації, оркестрації та взаємодії зі сторонніми сервісами.

Cortex XSOAR відрізняється тим, що має багато готових інтеграцій у своєму маркетплейсі та зручну вбудовану систему, яка допомагає легко впорядковувати й визначати типи інцидентів.Платформа підтримує тисячі конекторів, однак часто потребує складного налаштування та має високу вартість володіння, особливо за умов масштабування на великі SOC. IBM Resilient орієнтований на процесний менеджмент інцидентів і пропонує потужну модель workflow, але порівняно обмежену автоматизацію та меншу гнучкість у налаштуванні сценаріїв. Chronicle SOAR забезпечує швидку інтеграцію з Google Security Stack, проте має суттєво менше можливостей для глибокої кастомізації, а його функціональність більше орієнтована на невеликі та середні команди реагування.

Для порівняння функціональних можливостей провідних SOAR-рішень у таблиці 2 наведено характеристику їх переваг та обмежень.

Таблиця 2

Порівняльна характеристика провідних SOAR-платформ

Платформа	Сильні сторони	Обмеження та недоліки
Splunk Phantom	Підтримка Python-скриптів і кастомних інтеграцій; Широка модель containers/artifacts; Глибока інтеграція зі Splunk Enterprise; Висока швидкість виконання playbooks	Потребує більш кваліфікованих адміністраторів; Вища вартість у масштабних інсталяціях
Palo Alto Cortex XSOAR	Величезний маркетплейс інтеграцій; Потужний інтерфейс інцидент-менеджменту; Готові “incident types”	Висока ціна володіння; Значні витрати на налаштування; Залежність від екосистеми Palo Alto
IBM Resilient	Сильна модель workflow; Орієнтація на процесний менеджмент інцидентів; Добре підходить для регульованих галузей	Обмежена автоматизація; Менше можливостей кастомізації; Менша кількість інтеграцій
Google Chronicle SOAR (Siemplify)	Швидка інтеграція з Google Security Stack; Зручний інтерфейс Triage-центру; Низький поріг входу	Значно менше інтеграцій; Обмежені можливості глибокого кастомного сценарію; Орієнтований на менші SOC

У цьому контексті Splunk Phantom вирізняється поєднанням широких можливостей інтеграції, масштабованої обробки інцидентів та високого рівня автоматизації. Значною перевагою є підтримка Python-скриптів, що дозволяє створювати кастомні дії будь-якої складності, гнучка модель даних «containers/artifacts», а також тісна інтеграція з Splunk Enterprise для глибокої аналітики подій. Phantom також забезпечує високу швидкість виконання playbooks, прозорий аудит дій та можливість побудови комплексних багаторівневих сценаріїв реагування.

Порівняння провідних рішень демонструє що Splunk Phantom забезпечує найкраще співвідношення між гнучкістю, масштабованістю та функціональністю, що робить його раціональним вибором для сучасних SOC.

Архітектурні та функціональні переваги Splunk Phantom

Splunk Phantom вирізняється серед інших SOAR-платформ завдяки своїй гнучкій архітектурі, високій масштабованості та широким можливостям автоматизації, що робить його оптимальним рішенням для сучасних SOC-команд. Архітектурно Phantom побудований навколо моделі containers–artifacts, яка дозволяє структурувати всі дані інциденту у вигляді незалежних артефактів, зберігаючи повний контекст події та забезпечуючи гнучкість обробки. Такий підхід значно полегшує побудову сценаріїв реагування, оскільки кожний артефакт може бути використаний як вхідний параметр для подальших дій.

На рисунку 3 подано архітектуру взаємодії між Splunk Enterprise, Splunk Cloud та Splunk Phantom, яка демонструє процес формування, нормалізації й передачі подій у форматі CEF (Common Event Format) для подальшої автоматизованої обробки в SOAR-платформі [5, 6].

Ключовою перевагою платформи є можливість створення як стандартних, так і кастомних дій за допомогою Python-скриптів, що дозволяє інтегрувати практично будь-яку систему, сервіс або внутрішній інструмент компанії. Це забезпечує необмежену розширюваність та придатність для використання у складних корпоративних середовищах.

Широка бібліотека готових інтеграцій, що охоплює SIEM, EDR, IDS/IPS, хмарні сервіси та мережеве обладнання, гарантує швидке розгортання рішення без тривалих доопрацювань.

Функціональна частина Phantom підтримує високорівневі playbooks, побудовані за принципом графічних блоків дій. Це дозволяє аналітикам SOC створювати складні workflows без необхідності програмування, а технічним фахівцям – розширювати їх логіку при необхідності. Платформа також надає можливість паралельного виконання дій, умовних гілок, інтерактивних етапів та ручного втручання, що робить сценарії максимально адаптивними.

Тісна інтеграція зі Splunk Enterprise забезпечує ефективне використання аналітичних можливостей SIEM-платформи, включаючи кореляцію подій, побудову дашбордів та використання машинного навчання [6]. Крім того, Phantom пропонує розвинені засоби аудиту та документування інцидентів, що гарантує відповідність стандартам NIST та ISO.

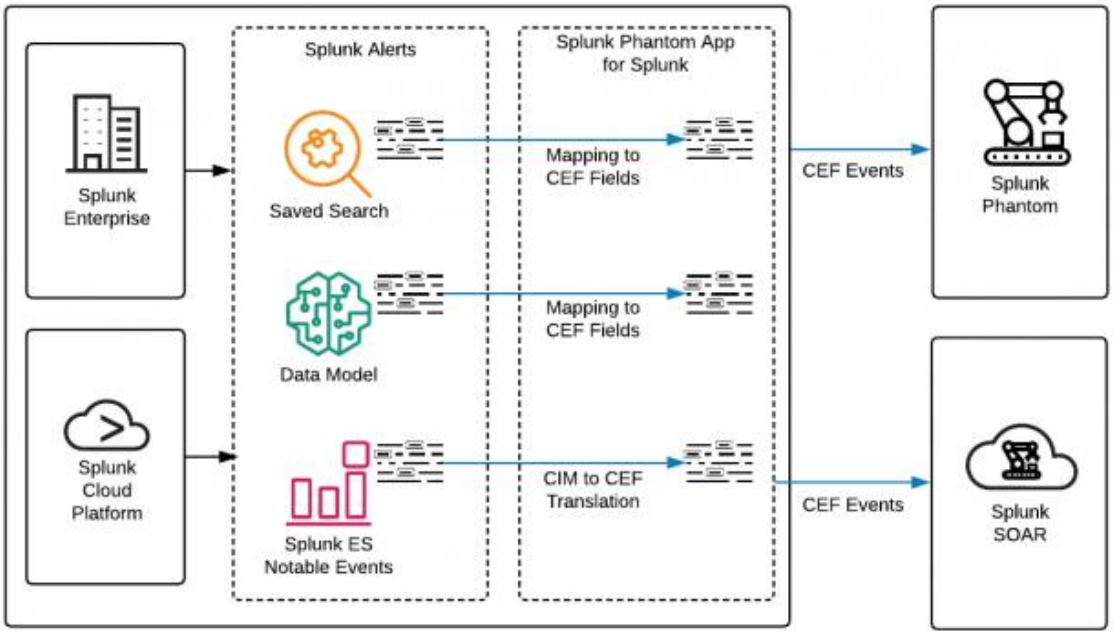

Рис. 3. Архітектура інтеграції Splunk Enterprise / Splunk Cloud із Splunk Phantom через CEF-події

У сукупності ці характеристики роблять Splunk Phantom одним із найбільш технічно досконалих і гнучких рішень для автоматизації реагування в SOC. Платформа забезпечує комплексний підхід до управління інцидентами, де високий рівень автоматизації поєднується з можливістю глибокої кастомізації та підтримкою будь-яких бізнес-процесів. Завдяки підходу «full lifecycle automation» Phantom охоплює всі етапи роботи з інцидентом – від первинного збору інформації, валідації та збагачення даних до локалізації загроз, виконання заходів з нейтралізації та формування детальної звітності. Додатковим фактором є масштабованість, яка дозволяє платформі рівномірно обробляти тисячі інцидентів без деградації продуктивності, що є критично важливим для великих корпоративних SOC із високою динамікою подій.

Phantom також забезпечує високий рівень прозорості та контрольованості процесів через розвинену систему логування, трекінгу змін та аудитних журналів, що спрощує процеси відповідності стандартам NIST, ISO 27035 та вимогам регуляторів. Гнучкий інтерфейс, можливість інтеграції з десятками зовнішніх джерел загроз, а також підтримка механізмів умовного прийняття рішень (human-in-the-loop) роблять платформу придатною як для повної автоматизації, так і для змішаних режимів роботи, де частина кроків контролюється аналітиком.

Використання Splunk Phantom дозволяє організаціям не лише прискорити та стандартизувати реагування, а й підвищити операційну стійкість SOC, суттєво зменшити навантаження на фахівців та забезпечити більш глибоку інтеграцію процесів безпеки у корпоративну інфраструктуру.

Висновки

У роботі проаналізовано роль SOAR-платформ у сучасних центрах моніторингу безпеки, що дозволяє зробити висновок про їхню ключову значущість для автоматизації рутинних процесів, зменшення впливу людського фактора та забезпечення структурованої обробки інцидентів за стандартними сценаріями реагування. Архітектура SOAR, яка включає інтеграційний, оркестраційно-аналітичний та операційний шари, дозволяє забезпечити повну взаємодію з зовнішніми системами безпеки, кореляцію подій, автоматизацію робочих процесів та контрольовану взаємодію аналітиків. Аналіз моделей автоматизації показав, що rule-based, state-based та context-aware підходи забезпечують різний рівень гнучкості та ефективності реагування на інциденти, причому context-aware автоматизація дозволяє оптимізувати пріоритетність інцидентів та зменшити кількість хибно-позитивних сповіщень.

Оцінка ефективності SOAR-систем базується на таких показниках, як MTTD, MTTR, Automation Coverage та False Positive Ratio, що дозволяє кількісно оцінити вплив платформи на продуктивність SOC, а методи тестування включають моделювання інцидентів та перевірку інтеграцій з зовнішніми системами. Порівняльний аналіз сучасних платформ показав, що Splunk Phantom вирізняється високою гнучкістю, масштабованістю та розвиненими можливостями автоматизації, що робить його оптимальним рішенням для великих корпоративних SOC. Особливості Splunk Phantom включають модель containers-artifacts, підтримку кастомних дій через Python, графічні playbooks, паралельне виконання задач та інтеграцію зі Splunk Enterprise, що забезпечує повний цикл автоматизованого реагування – від збору та збагачення даних до локалізації загроз, усунення наслідків та формування детальної звітності. Використання SOAR дозволяє підвищити ефективність роботи SOC, стандартизувати процеси реагування, зменшити навантаження на фахівців та інтегрувати безпекові процеси у корпоративну інфраструктуру.

Список використаної літератури

1. Kovacevic B. Оркестрація безпеки, автоматизація та реагування для аналітиків безпеки: дізнайтеся секрети SOAR для покращення MTTA і MTTR та зміцнення рівня безпеки. Packt Publishing, Limited, 2023.
2. Marlette T. Найкращі практики Splunk. Packt Publishing, Limited, 2016.
3. Pitkar H. Автоматизація хмарної безпеки через Symmetry: виявлення та реагування на загрози. Symmetry. 2025. Vol. 17, no. 6. P. 859. URL: https://doi.org/10.3390/sym17060859 (дата звернення: 21.11.2025).
4. Тестування SOAR-інструментів у практичному використанні / R. A. Bridges et al. Computers & Security. 2023. P. 103201. URL: https://doi.org/10.1016/j.cose.2023.103201 (дата звернення: 21.11.2025).
5. До надійної оркестрації безпеки та автоматизованого реагування в центрах операцій безпеки: гіперавтоматизаційний підхід із використанням агентного штучного інтелекту / Ismail et al. Information. 2025. Vol. 16, no. 5. P. 365. URL: https://doi.org/10.3390/info16050365 (дата звернення: 21.11.2025).
6. Москвін К.С., Сєвєрінов О.В., Сидоренко З.М., Балагура Д.С., Литвин А.В. Дослідження впливу інтеграції засобів кіберзахисту на захищеність ІТ-інфраструктури організації. Том 2 № 2(93) (2025): Вісник Херсонського національного технічного університету. С. 246-255. DOI: https://doi.org/10.35546/kntu2078-4481.2025.2.2.29

References

1. Kovacevic B. (2023) Security Orchestration, Automation and Response for Security Analysts: Learn the Secrets of SOAR to Improve MTTA and MTTR and Strengthen Your Security Posture. Packt Publishing, Limited.
2. Marlette T. (2016) Splunk Best Practices. Packt Publishing, Limited.
3. Pitkar H. (2025) Cloud Security Automation Through Symmetry: Threat Detection and Response. Symmetry. Vol. 17, no. 6. P. 859. URL: https://doi.org/10.3390/sym17060859 (date of access: 23.11.2025).
4. Bridges R. A. et al. Computers & Security (2023) Testing SOAR Tools in Use. P. 103201. URL: https://doi.org/10.1016/j.cose.2023.103201 (date of access: 21.11.2025).
5. Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence / Ismail et al. Information. 2025. Vol. 16, no. 5. P. 365. URL: https://doi.org/10.3390/info16050365 (date of access: 22.11.2025).
6. Moskvin K.S., Sievierinov O.V., Sydorenko Z.M., Balagura D.S., Lytvyn A.V. (2025) Research on the Impact of Cybersecurity Tools Integration on the Security of an Organization's IT Infrastructure. Visnyk of Kherson National Technical University. Vol. 2, No. 2(93). P. 246-255. DOI: https://doi.org/10.35546/kntu2078-4481.2025.2.2.29

Дата першого надходження рукопису до видання: 26.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025