ВИКОРИСТАННЯ SPLUNK SOAR PHANTOM ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА ІНЦИДЕНТИ В SOC

Мартиненко Я.А., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Центри операцій безпеки SOC щоденно отримують та обробляють велику кількість кіберінцидентів, що часто може подовжити час реагування та підвищити ймовірність пропуску загроз, які можуть спричинити значні наслідки для організації. За результатами SANS Institute, приблизно 79% центрів операцій безпеки функціонують у режимі 24/7, що свідчить про потребу у постійному моніторингу інформаційної інфраструктури та миттєвому реагуванні на інциденти безпеки [1]. Співробітники SOC формують звіти власноруч, витрачаючи на це значну частину робочого дня. У той час автоматизація залишається обмеженою, що створює потенціал для впровадження платформ типу SOAR для підвищення ефективності [2, 3].

Метою доповіді є дослідження можливостей платформи Splunk SOAR Phantom для автоматизації процесу реагування на інциденти в SOC та оцінки ефективності її використання з метою оптимізації часу та ресурсів обробки інцидентів.

Згідно зі звітом Gartner Market Guide for Security Orchestration, Automation and Response Solutions [4] ринок SOAR рішень нині перебуває у фазі активного злиття з SIEM-платформами, формуючи єдині системи управління та реагування на інциденти. Такий підхід забезпечує підвищення ефективності роботи SOC шляхом об’єднання процесів моніторингу, аналітики та автоматизації реагування. У переліку провідних продуктів ринку Gartner [4] виокремлює Splunk SOAR, який демонструє інтеграційні можливості та розширену взаємодію з джерелами загроз і зовнішніми API.

Саме тому у ході було реалізовано інтеграцію між Splunk SOAR Phantom [5] та SIEM-системою Splunk Enterprise Security [6], що робить їхню взаємодію ефективним інструментом для оптимізації та автоматизації реагування на інциденти у середовищі SOC. Така взаємодія забезпечує автоматичне отримання повідомлень алертів із SIEM і подальшу обробку інцидентів за допомогою заздалегідь впроваджених сценаріїв плейбуків.

Крім того, значним напрямом розвитку є покращення здатності Splunk SOAR працювати разом з іншими аналітичними платформами та хмарними сервісами. Це дасть змогу об’єднати всі системи безпеки в одну узгоджену екосистему, де дані аналізуватимуться централізовано, а реагування на загрози відбуватиметься швидше та ефективніше. Наприклад, у дослідженні було обрано API-платформу AbuseIPDB, яка дозволяє виконувати перевірку статусів і репутації IP-адрес. Після надходження оповіщення про підозрілу IP-адресу з SIEM, система SOAR автоматично витягує цю адресу з події, надсилає запит до AbuseIPDB API та отримує звіт про репутацію. У разі виявлення підозрілої активності SOAR додатково перевіряє наявність цієї IP-адреси у внутрішньому “чорному списку” організації. Якщо збігів не виявлено, плейбук

автоматично формує повідомлення для працівників SOC із рекомендацією щодо блокування IP-адреси.

Доцільно використовувати технології машинного навчання для підвищення точності автоматичного визначення рівня важливості інцидентів і вдосконалення механізмів кореляції подій між різними джерелами даних, що дозволить ще більше скоротити час реагування та зменшити кількість хибних спрацювань. Впровадження інтелектуальних алгоритмів аналізу загроз дозволить автоматично виявляти складні атаки, що часто залишаються непоміченими при традиційних методах моніторингу.

У доповіді наводяться результати вимірювань ефективності впровадження автоматизованого реагування на інциденти за допомогою Splunk SOAR Phantom. Спираючись на них, можна стверджувати, що реалізована інтеграція дозволяє працівникам SOC-центрів мінімізувати обсяг ручної обробки подій, яка інколи може призводити до затримок у реагуванні більш серйозних подій. Згідно з результатами дослідження компанії Exaforce [2], впровадження автоматизації реагування дає змогу скоротити час розслідування інцидентів більш ніж на 60 %. Тож, подальший розвиток таких систем передбачає вдосконалення взаємодії між людиною та автоматизованими механізмами реагування. Це дає змогу зменшити навантаження на аналітиків SOC, скоротити час ухвалення рішень і мінімізувати вплив людського фактора на процес реагування.

Отже, інтеграція Splunk SOAR Phantom із Splunk Enterprise Security на практиці показує, як можна автоматизувати та узгодити процеси кіберзахисту. Використання SOAR-рішень є ефективним способом створення сучасної та гнучкої системи реагування на інциденти безпеки, яка відповідає поточним вимогам і тенденціям розвитку кібербезпеки.

Список літератури

1. *Elastic – The Search AI Company | Elastic*. URL: https://www.elastic.co/pdf/sans-soc-survey-2025.pdf (дата звернення: 05.11.2025).

2. Exaforce Learning Center | Automating incident response in the SOC: Machine-speed defense for modern threats. *Exaforce*. URL: https://www.exaforce.com/learning-center/automating-incident-response-in-the-soc-machine-speed-defense-for-modern-threats?utm_source=chatgpt.com (дата звернення: 05.11.2025).

3. Ушатов, В., Сєвєрінов, О.В. (2019). Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки.

4. Security Orchestration, Automation and Response Solutions Reviews and Ratings. *www.gartner.com*. URL: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions (дата звернення: 05.11.2025).

5. *Splunk SOAR Validated Architectures Version 2.0| The Key to Enterprise Resilience*. URL: https://www.splunk.com/en_us/pdfs/tech-brief/splunk-phantom-validated-architectures.pdf (дата звернення: 05.11.2025).

6. Splunk® Enterprise Security Analytics Driven Security and Continuous Monitoring for Modern Threats. *Winncom Technologies | Головна*. URL: https://winncom.ua/wp-content/uploads/2018/07/Splunk-Enterprise-Security.pdf (дата звернення: 05.11.2025).