УДК 004.738.5

Ковальчук О.М., здобувач
Колощук М.С., ст. викладач
Дячук О.Ю., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ВИКОРИСТАННЯ SOAR-ПЛАТФОРМ ДЛЯ АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

У сучасних умовах стрімкого зростання кількості кіберзагроз ефективність реагування на інциденти інформаційної безпеки стає одним із ключових факторів забезпечення стійкості IT-інфраструктури. Традиційні підходи до обробки подій безпеки, що базуються переважно на ручному аналізі, не забезпечують необхідної швидкості реагування та створюють значне навантаження на фахівців центрів моніторингу безпеки [1].

Метою даної роботи є аналіз можливостей застосування платформ класу SOAR (Security Orchestration, Automation and Response) для підвищення ефективності процесів виявлення та реагування на кіберінциденти.

Платформи SOAR призначені для інтеграції різнорідних інструментів інформаційної безпеки, автоматизації типових сценаріїв реагування та централізації управління інцидентами [2]. На відміну від класичних систем моніторингу, SOAR-рішення дозволяють не лише агрегувати події, але й виконувати автоматизовані дії у відповідь на виявлені загрози.

Ключовим елементом SOAR є механізм оркестрації, що забезпечує взаємодію між різними системами захисту, такими як SIEM, IDS/IPS, антивірусні рішення та системи контролю доступу. Обмін даними між компонентами реалізується через програмні інтерфейси (API), що дозволяє формувати єдине середовище обробки інцидентів [1].

Важливу роль у функціонуванні SOAR відіграють плейбуки — формалізовані сценарії реагування на типові загрози. Вони визначають послідовність дій, які виконуються автоматично або з частковим залученням аналітика, що дозволяє стандартизувати процеси реагування та зменшити кількість помилок [2].

Окрім цього, SOAR-платформи забезпечують централізоване управління інцидентами, що спрощує координацію дій між різними підрозділами та підвищує прозорість процесів інформаційної безпеки.

Структуру взаємодії основних компонентів SOAR-платформи наведено на рис. 1.

Рис. 1. Узагальнена схема функціонування SOAR-платформи

Практичне застосування SOAR-платформ включає автоматизацію реагування на типові інциденти, зокрема фішингові атаки, виявлення шкідливого програмного забезпечення та несанкціонований доступ. У таких випадках система може автоматично перевіряти індикатори компрометації, блокувати облікові записи та ізолювати скомпрометовані вузли.

Особливо ефективним є використання SOAR у поєднанні з системами класу SIEM, які здійснюють збір та кореляцію подій безпеки. У такому випадку SIEM виступає джерелом подій, тоді як SOAR забезпечує автоматизовану обробку інцидентів і виконання відповідних дій реагування. Такий підхід дозволяє значно скоротити час від виявлення загрози до її нейтралізації.

На відміну від традиційних підходів, що потребують значної участі аналітика, SOAR дозволяє автоматизувати більшість процесів реагування та забезпечує їх стандартизацію через використання плейбуків, що зменшує затримки та мінімізує помилки.

У результаті аналізу встановлено, що використання SOAR-рішень дозволяє:

- суттєво скоротити час реагування на інциденти;
- знизити навантаження на аналітиків SOC;
- підвищити узгодженість і повторюваність процесів;
- покращити інтеграцію між засобами захисту.

Разом з тим, впровадження SOAR супроводжується рядом обмежень, зокрема необхідністю попередньої інтеграції систем, складністю розробки ефективних плейбуків та потребою у кваліфікованому налаштуванні [2].

Таким чином, застосування SOAR-платформ є перспективним напрямом розвитку систем кібербезпеки, що забезпечує підвищення ефективності реагування на інциденти за умови належного налаштування та інтеграції.

Список використаних джерел

1. IBM Security. *What is SOAR (Security Orchestration, Automation and Response)?* URL: https://www.ibm.com/topics/soar

Microsoft Security. *What is SOAR?* URL: https://www.microsoft.com/security/business/security-101/what-is-soar