УДК 004.7

Єфіменко А. А., здобувач,
Єфіменко А.А., к.т.н., доцент,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

МОДЕЛЬ ПОБУДОВИ SOC З ВИКОРИСТАННЯМ ІНТЕГРАЦІЙ ВІДКРИТИХ ПРОГРАМНИХ РІШЕНЬ

У сучасних умовах стрімкого розширення цифрового простору та зростання інтенсивності кіберзагроз особливої актуальності набуває формування ефективних механізмів забезпечення інформаційної безпеки. Збільшення технологічного периметру, розвиток розподілених інфраструктур та зростання кількості векторів атак вимагають постійного моніторингу подій безпеки та оперативного реагування на інциденти. Операційні центри безпеки (SOC) є ключовими елементами такої інфраструктури, проте традиційні комерційні рішення залишаються недоступними для значної частини малих і середніх організацій через високу вартість впровадження та підтримки. У цьому контексті використання відкритих програмних рішень є перспективним напрямом, що забезпечує можливість створення адаптивних, масштабованих і економічно доцільних моделей SOC.

Аналіз наукових і технічних джерел свідчить про зростаючий інтерес до застосування інструментів із відкритим кодом для логування, аналізу подій, управління інцидентами та автоматизації реагування. Разом з тим, у науковій літературі недостатньо представлено комплексні підходи до побудови SOC на основі повністю відкритого технологічного стеку. Потребують уточнення питання інтеграції компонентів різного призначення, узгодження архітектурних принципів їх взаємодії, формалізації інформаційних потоків та визначення моделей, що описують структурну та функціональну організацію процесів моніторингу і реагування. На практичному рівні існує дефіцит методичних рекомендацій щодо впровадження SOC в умовах обмежених ресурсів і відсутності стандартизованих технологічних підходів.

Метою роботи є розроблення моделі SOC із використанням відкритих рішень, визначення її архітектурних характеристик та побудова прототипу, який забезпечує виявлення, кореляцію та автоматизоване реагування на інциденти інформаційної безпеки. Основна ідея полягає у створенні концептуальної моделі, що інтегрує функціональні можливості відкритих систем SIEM, SOAR та IR у єдине середовище моніторингу та реагування, а також у формулюванні

положень, які визначають функціональні взаємозв'язки компонентів SOC та логіку їх взаємодії в межах цілісної архітектури.

Дослідження виконано в лабораторному середовищі на базі VirtualBox з використанням програмних рішень Wazuh, TheHive, Cortex та Shuffle. Архітектура моделі ґрунтувалася на узгодженні процесів аналізу телеметрії, обробки інцидентів та реалізації автоматизованих реакцій. Для теоретичного обґрунтування використовувалися методики структурного аналізу, системного підходу та моделювання типових сценаріїв загроз, що визначаються за MITRE ATT&CK.

Отримані результати дозволили узагальнити принципи побудови SOC на основі відкритих технологій, визначити архітектурні та функціональні параметри інтегрованої системи, а також сформулювати положення, які описують логіку організації потоків даних і взаємодії між основними підсистемами. Практичне значення дослідження полягає у можливості застосування розробленої моделі для створення доступних рішень у сфері кіберзахисту, формування навчальних і тренувальних середовищ, а також у використанні отриманих результатів як методичної бази для впровадження SOC у організаціях різного масштабу.

Таким чином, використання відкритих програмних рішень може слугувати ефективною основою для побудови доступного SOC, що забезпечує базову автоматизацію, зниження вартості впровадження та адаптованість до потреб організацій. Перспективи подальших досліджень включають розроблення контейнеризованих рішень для розгортання SOC, інтеграцію механізмів машинного навчання для виявлення аномалій та удосконалення автоматизованих сценаріїв реагування.

Список використаних джерел:

1. MITRE. 11 Strategies of a World-Class Cybersecurity Operations Center. 2022. 452 с

2. AT&T Business. How to Build a Security Operations Center (on a Budget). 2019. 35 с.