УДК 004.056:004.7

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПРОЦЕСІВ АВТОМАТИЗАЦІЇ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ У ХМАРНИХ СЕРЕДОВИЩАХ

Фісенко Д.М., Білодід В.Г.
e-mail: dmytro.fisenko@nure.ua, e-mail: vibos111@gmail.com
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна,
Харківський університет повітряних сил ім.І.Кожедуба
м. Харків, Україна

This work is devoted to determining the features of implementing security orchestration, automation and response approach. The main features and benefits of the approach were considered. The combination of SOAR and Machine Learning (ML) is critical to modern cybersecurity, enabling organizations to respond to threats faster, manage incidents more effectively, and improve the accuracy of anomaly detection.

Забезпечення інформаційної безпеки в хмарних середовищах складається з багатьох аспектів. Важливими є вчасне реагування на загрози та автоматизація процесів, щоб зменшити вплив людського фактору. Впровадження систем оркестрації, автоматизації й реагування (SOAR) є значущим етапом у цьому процесі. Даний підхід включає в себе набір технологій що дозволяють ефективніше управляти процесами інформаційної безпеки за рахунок агрегації вхідних даних з різних джерел, автоматизації повсякденних завдань та централізованого реагування на інциденти.

Головними задачами впровадження SOAR є забезпечення оркестрації, автоматизації та управління і реагування на інциденти. При вирішенні задачі оркестраії головною метою є об’єднання та узгодження роботи всіх систем які відповідають за інформаційну безпеку. На цьому етапі відбувається інтеграція таких систем як сканери вразливостей брандмауери, системи виявлення та запобігання вторгненням тощо, в єдиний інтерфейс за допомогою якого можна централізовано керувати процесами в різних продуктах безпеки [1].

Наступним є вирішення задачі автоматизації. На цьому етапі головною метою є розробка та впровадження скриптів та утиліт які дозволять автоматизувати виконання завдань які раніше виконувались виключно спеціалістами з інформаційної безпеки. При вирішенні цієї задачі великий акцент робиться на використання машинного навчання, оскільки за його допомогою є можливість перевірити великі об’єми даних для виявлення тенденції які можуть вказувати на загрозу в безпеці.

Остання задача яка вирішується за допомогою SOAR підходу це процес реагування. Якщо на етапі оркестрації відбуваєтья обєднання джерел

даних, а на етапі автоматизації прибираються процеси які виконувались вручну то на етапі реагування акцент ставиться на безпосередньому вживанні заходів, що зупинять чи зведуть до мінімуми шкоду від інциденту. При цьому розробляються процедури які, у разі виявлення інциденту, дозволять провести координоване знешкодження загрози інформаційної безпеки. Наприклад ізоляція компрометованих серверів, блокування облікових записів тощо [2].

Використання даного підходу має багато переваг. Завдяки процесам оркестрації та автоматизації є можливим значно скоротити час виявлення на знешкодження загрози інформаційної безпеки. Також зменшується кількість дій які необхідно виконувати вручну. Завдяки агрегації даних створюється єдине джерело правди що дає змогу покращити аналіз вхідної інформації. Також, завдяки модульній архітектурі є можливість інтегрувати нові безпекові технології та джерела даних.

Слід зазначити, що оскільки даний підхід використовує машинне навчання для аналізу даних, велику увагу слід приділяти даним які використовуються для навчання моделі машинного навчання та вибору алгоритму. При навчанні моделі слід використовувати достатні об’єми даних для забезпечення точного результату.

Список використаних джерел:

1. Jangampet, Vinay Dutt. (2024). CYBERSECURITY EVOLUTION MODEL: AI/ML IN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE. 15. 1-6.

2. Jangampet, Vinay Dutt & Pulyala, Srinivas & Desetty, Avinash Gupta. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 10. 1545-1549. 10.61841/turcomat.v10i3.14323.