АНАЛІЗ ПРАВИЛ КОРЕЛЯЦІЇ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ПОДІЯМИ БЕЗПЕКИ

Овчаренко М.Ю., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день системи управління інформаційною безпекою та подіями безпеки (Security Information and Event Management, SIEM) є одними з найрозповсюдженіших систем управління інцидентами інформаційної безпеки тому, що вони здатні обробляти великі обсяги інформації про події в інформаційній системі від різних джерел в режимі реального часу та інформувати адміністратора про появу інцидентів інформаційної безпеки [1]. Проте кожен день в інформаційних системах відбуваються сотні та навіть тисячі подій, більшість з яких є результатами нормального функціонування системи та її користувачів, тож потрібно розробляти та впроваджувати правила, які будуть відділяти звичайні системні події від інцидентів безпеки, так звані правила кореляції.

Метою доповіді є аналіз існуючих правил кореляції в системах управління інформаційною безпекою та подіями безпеки та вибір оптимальних правил кореляції для використання в сучасних інформаційно-телекомунікаційних систем.

В доповіді були розглянуті існуючі правила кореляції, які можна об'єднати в дві групи – сигнатурні та несигнатурні. Несигнатурні правила, так звані «правила з коробки», розробляються постачальниками SIEM-систем та їх неможливо видозмінити, до них можна віднести статистичні правила, на графах, на нейронних мережах. На відміну від несигнатурних сигнатурні правила можливо видозмінити, що робить їх більш гнучкими та ефективними. До таких можна віднести кількісні (реагування на інцидент в залежності від кількості його появ в системі) та ймовірнісні (реагування на інцидент в залежності від ймовірності його появи в системі) [2, 3]. Таким чином впровадження правил кореляції в SIEM-систему призводить до зменшення часу реагування на інциденти та негативних наслідків, які можуть бути нанесені системі та її власникам, а використання сигнатурних правил дозволяє точніше налаштувати SIEM-систему під певні потреби та підвищити її керованість.

Список літератури

1. Ушатов В., Сєвєрінов О.В.. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105. (2019).

2. Sievierinov O.V., Ovcharenko M.Y. Analysis of correlation rules in Security information and event management systems. *Computer and information systems and technologies*. 2020. P. 24-25.

3. Miller D. et al. Security information and event management (SIEM) implementation. – McGraw-Hill, 2011.