ВІДПОВІДНІСТЬ SIEM ELASTIC ВИМОГАМ ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035

Туз М.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

SIEM-рішення (Security Information and Event Management) дозволяють об'єднати в єдину платформу збір, кореляцію, аналіз та зберігання даних про події в мережі, допомагаючи виявляти потенційні загрози та ефективно реагувати на них. Вони є ключовим компонентом сучасних стратегій кібербезпеки, надаючи можливість не лише запобігати атакам, але й зменшувати їхній вплив [1, 2].

Elastic, один із популярних інструментів SIEM, пропонує комплексне рішення для моніторингу та аналізу даних, забезпечуючи масштабованість, високу продуктивність і функціональність. Завдяки можливості автоматизації збору, аналізу, збереження логів та моніторингу подій безпеки, SIEM Elastic сприяє виявленню загроз, реагуванню на інциденти та забезпеченню збереження доказів [3].

Метою доповіді є аналіз особливостей роботи SIEM-рішень, зокрема Elastic, оцінка їхніх можливостей у виявленні загроз та атак, а також визначення їх відповідності вимогам міжнародних стандартів інформаційної безпеки, таких як ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035 [4]. В доповіді надані результати аналізу та дослідження основних можливостей та функціоналу платформи Elastic, принципів її роботи та застосування.

Основний функціонал Elastic забезпечує гнучкий підхід до збору, обробки, аналізу та візуалізації даних, що робить цю платформу універсальним інструментом для моніторингу та забезпечення безпеки. Максимальна ефективність цього інструменту залежить від кваліфікації та досвіду персоналу. Успіх у реагуванні на інциденти та виявленні потенційної загрози чи спроби несанкціонованого доступу значною мірою визначається рівнем обізнаності користувачів, їх здатністю правильно налаштовувати правила та інтерпретувати отриману інформацію. Впровадження SIEM-рішення Elastic дозволить організаціям ефективно реалізовувати вимоги міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035, забезпечуючи належний рівень управління інформаційною безпекою.

Список літератури

1. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ" ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.

2. Сєвєрінов О.В., Ушатов В.В. Управління інцидентами інформаційної безпеки на основі використання SIEM систем. (2019).

3. Marco Mancini. Security analytics with Elastic. openaccess.uoc.edu:веб-сайт. URL: http://surl.li/hfdbus.

4. Сєвєрінов О.В., Черниш В.І., Молчанова М.Є. Управління інформаційною безпекою згідно міжнародних стандартів // Системи управління, навігації та зв'язку.– К: ДП «ЦНДІ НіУ».-2011.–Вип 4.20 (2011): 250-253.