Колощук М. С., магістрантка, гр. КБм-21-1
Єфіменко А. А., к.т.н., доц.,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Вакалюк Т. А., д.пед.н., проф.,
професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

УНІВЕРСАЛЬНИЙ ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ — СИСТЕМА SIEM

Системи інформаційної безпеки, що включають моніторинг, кореляцію подій, пов'язаних з будь-яким об'єктом, повідомленнями та виведенням інформації на кінцеві пристрої під управлінням адміністратора, називають Security event management, а системи, що відповідають за зберігання, звітність та аналіз акумульованих даних, – Security information management. Поняття SIEM включає обидва ці аспекти, об'єднує їх у єдиній системі і надає централізоване управління обома областями [2].

Інструменти SIEM забезпечують:

1) видимість у реальному часі систем інформаційної безпеки організації.
2) керує журналом подій, що об'єднує дані з багатьох джерел.
3) кореляція подій, зібраних із різних журналів або джерел безпеки, з використанням правил «якщо», які додають інтелектуальності необробленим даним.
4) автоматичні сповіщення про події безпеки. Більшість систем SIEM надають панелі моніторингу проблем безпеки та інших методів прямого повідомлення.
5) SIEM працює шляхом об'єднання двох технологій: a) управління інформацією про безпеку (SIM), яке збирає дані з файлів журналів для аналізу та звітів про загрози та події безпеки; та b) управління подіями безпеки (SEM), яке проводить моніторинг системи в реальному часі . повідомляє адміністраторів мережі про важливі проблеми та встановлює кореляцію між подіями безпеки [1].

Інформацію про безпеку та процес управління подіями можна розбити таким чином:

1) збір даних – всі джерела інформації про мережеву безпеку, наприклад, сервери, операційні системи, брандмауери, антивірусне програмне забезпечення та системи запобігання вторгненням, налаштовані для передачі даних про події інструментом SIEM. Більшість сучасних інструментів SIEM використовують агентів для збору журналів подій із корпоративних систем, які потім обробляються, фільтруються та відправляються до SIEM. Деякі SIEM допускають збирання даних без агентів. Наприклад, Splunk пропонує безагентний збір даних у Windows за допомогою WMI.
2) політики – профіль створюється адміністратором SIEM, який визначає поведінку корпоративних систем як у нормальних умовах, так і заздалегідь визначених інцидентів безпеки. SIEM надають правила, попередження, звіти та інформаційні панелі за замовчуванням, які можна настроювати та настроювати відповідно до конкретних потреб безпеки.
3) консолідація та кореляція даних – рішення SIEM поєднують, аналізують та аналізують файли журналів. Потім події класифікуються на основі необроблених даних та застосовуються правила кореляції, які поєднують окремі події даних у значущі проблеми безпеки.
4) повідомлення – якщо подія або набір подій запускають правило SIEM, система повідомляє персонал служби безпеки [1].

За допомогою SIEM можна досягти майже абсолютної автоматизації процесу виявлення загроз. При коректному впровадженні такої системи підрозділ інформаційної безпеки переходить абсолютно новий рівень надання сервісу. SIEM дозволяє акцентувати увагу лише на критичних та дійсно важливих загрозах, працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії та ризики, запобігати фінансовим втратам та підвищувати ефективність та безпеку роботи компанії загалом [2].

Список використаних джерел

1. Gustavo Gonzalez-Granadillo, Susana González-Zarzosa and Rodrigo Diaz Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 2021. 33 с.

David Swift A Practical Application of SIM/SEM/SIEM Automating Threat Identification, 2021. 40 с.