СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ПРО БЕЗПЕКУ ТА УПРАВЛІННЯ ПОДІЯМИ

Софія Довганик, Орест Полотай
Національний університет «Львівська політехніка»

Описано основне призначення та особливості SIEM-систем для збору інформації та управління подіями. Показано основні джерела інформації, які використовуються для таких систем. Наведено перелік сучасних SIEM-систем.

Ключові слова: захист інформації, SIEM-системи, управління подіями.

The main purpose and features of SIEM systems for information gathering and event management are described. The main sources of information used for such systems are shown. The list of modern SIEM-systems is given.

Keywords: information security, SIEM systems, event management.

Оскільки практично більшість підприємств працюють в Інтернеті, все важливіше використовувати інструменти кібербезпеки та виявлення загроз для запобігання простоїв роботи. На жаль, у мережі багато активних недобросовісних зловмисників, які лише чекають удару по вразливих системах. Інформація про безпеку та управління подіями (SIEM) стали основною частиною виявлення та подолання кібератак.

Системи захисту, відомі під абревіатурою SIEM, з'явилися в результаті еволюції і злиття SEM і SIM.

SEM – Security Event Management – система захисту, яка працює в режимі реального часу. Вона самостійно спостерігає за подіями в інформаційних потоках, збирає їх, виробляє кореляцію і генерує превентивні повідомлення.

SIM – Security Information Management – система, яка відповідає за аналіз відомостей на основі статистики та девіацій від встановлених правил безпеки.

Абревіатура SIEM означає «Система Збору та Кореляції Подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому – аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів і призначених для користувача ПК, і при цьому детектувати відхилення від норм по якимось критеріям. Якщо таке відхилення виявлено – система генерує інцидент. Варто відзначити, що в основі роботи SIEM лежать, в основному, статистичні та математичні технології, схожі на ті, що використовуються, наприклад, в BI-системах.

До речі, SIEM-система не тільки автоматизує аналіз різних системних подій. Важливо, що з її допомогою можна виявити дії, які зовні виглядають цілком нешкідливими, але в сукупності становлять загрозу. Наприклад, якщо довірений користувач відправляє конфіденційні дані на email-адресу, що лежить поза звичного кола адресатів, то DLP-система не завжди відловлює такі дії, проте SIEM згенерує інцидент на базі накопиченої статистики.

Діапазон завдань, які здатна вирішити SIEM-система, дійсно дуже широкий. По-перше, про що вже згадувалося раніше, це автоматизація моніторингу та аналізу всіх подій, які відбуваються в численних системах захисту. Друге важливе завдання, цілей, заради якої використовуються SIEM-технології: в разі інциденту SIEM здатна надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду. Третє важливе призначення системи – SIEM допомагає проводити аудити на відповідність різним галузевим стандартам.

Більше число джерел даних означає більш повне і ретельне охоплення всіх подій, що реєструються в IT-інфраструктурі підприємства. Для виконання свого завдання сучасні SIEM-системи використовують такі джерела інформації:

- ***Access Control, Authentication.*** Застосовуються для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- ***DLP-системи.*** Відомості про спроби інсайдерських витоків, порушення прав доступу.

- ***IDS / IPS-системи.*** Несуть дані про мережеві атаки, зміни конфігурації і доступу до пристроїв.
- ***Антивірусні програми.*** Генерують події про працездатність ПО, базах даних, зміні конфігурацій і політик, шкідливий код.
- ***Журнали подій серверів і робочих станцій.*** Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- ***Міжмережеві екрани.*** Відомості про атаки, шкідливі програми та інше.
- ***Мережеве активне обладнання.*** Використовується для контролю доступу, обліку мережевого трафіку.
- ***Сканери вразливостей.*** Дані про інвентаризацію активів, сервісів, ПО, вразливостей, поставка інвентаризаційних даних і топологічної структури.
- ***Системи інвентаризації та asset-management.*** Поставляють дані для контролю активів в інфраструктурі і виявлення нових.
- ***Системи веб-фільтрації.*** Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів.

SIEM-системи стали основним компонентом безпеки сучасних організацій. Основна причина полягає в тому, що кожен користувач або трекер залишає після себе віртуальний слід у даних журналу мережі. Системи SIEM розроблені для використання цих даних журналу, щоб генерувати уявлення про минулі атаки та події. Система SIEM не тільки визначає, що стався напад, але дозволяє вам бачити, як і чому це сталося.

По мірі того, як організації оновлюють і покращують масштабність все більш складних IT-інфраструктур, SIEM набуває ще більшого значення в останні роки. Всупереч поширеній думці, брандмауерів та антивірусних пакетів недостатньо для захисту мережі в цілому. Нульові атаки все ще можуть проникнути в захисні сили системи навіть при застосуванні цих заходів безпеки.

Серед сучасних SIEM систем, варто виділити такі:

- ManageEngine EventLog Analyzer;
- Журнал SolarWinds & Менеджер подій;
- IBM Security QRadar.

Використання SIEM також допомагає компаніям дотримуватися різноманітних галузевих правил управління інформаційною безпекою. Системи SIEM забезпечують найкращий спосіб задоволення цієї нормативної вимоги та забезпечують прозорість журналів, щоб генерувати чітку інформацію та вдосконалення.

Список використаної літератури

1. Столова О. В. Методика порівняння ефективності сучасних SIEM-систем: [Електронний ресурс]. – Режим доступу: http://ela.kpi.ua/bitstream/123456789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0.163-164.pdf

2. TIM KEARY 9 Best SIEM Tools: A Guide to Security Information and Event Management. [Електронний ресурс]. – Режим доступу: https://www.comparitech.com/net-admin/siem-tools/

3. Drew Robb, Top SIEM Products [Електронний ресурс]. – Режим доступу: https://www.esecurityplanet.com/products/top-siem-products.html

4. Abhishek Sharma, Senior Technical Marketing Engineer at Securonix The Anatomy of a Modern SIEM: https://www.securonix.com/the-anatomy-of-a-modern-siem/