УДК 681.3.06

Р. Козак
(Тернопільський національний технічний університет імені Івана Пулюя)

СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ

Виникнення нових видів загроз змушує розробників систем захисту адаптувати свої продукти до актуальних обставин. Крім цього, кількість джерел інформації, з яких надходять дані про поточний стан захищеності, зростає з кожним днем. Коли інфраструктура занадто складна, неможливо встежити за загальною картиною того, що в ній відбувається. Якщо вчасно не реагувати на виникаючі загрози та запобігати їм, користі не буде навіть від сотні систем виявлення атак. Виходом із цієї ситуації безсумнівно є системи Security Information and Event Management (SIEM).

Перед системою SIEM ставляться наступні завдання:

- консолідація та зберігання журналів подій від різних джерел – мережних пристроїв, додатків, журналів ОС, засобів захисту тощо;
- надання інструментів для аналізу подій і розбору інцидентів;
- кореляція та обробка за правилами;
- автоматичне оповіщення й інцидент-менеджмент.

Система SIEM є універсальною за рахунок своєї логіки. Для вирішення покладених на SIEM завдань необхідні достовірні джерела інформації та правила кореляції.

SIEM здатна виявляти:

- мережні атаки у внутрішньому й зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження, «бекдори» і троянці;
- спроби несанкціонованого доступу до конфіденційної інформації;
- помилки та збої в роботі інформаційних систем;
- вразливості;
- помилки конфігурацій у засобах захисту й інформаційних систем.

Реєстрація інцидентів у власній або зовнішній системі HelpDesk відіграє важливу роль. По-перше, це документування виникаючих інцидентів. Якщо є зареєстрований інцидент, тобто й відповідальний за його вирішення, є терміни. Інцидент не залишиться неврахованим (як це буває у випадку оповіщення по електронній пошті). По-друге, це статистика по інцидентах, що дозволяє виявляти проблеми (однотипні інциденти, що повторюються часто й закриті без усунення істинних причин). На підставі статистики і розрахунку основних показників можна також судити про ефективність роботи окремих співробітників, підрозділу ІБ, засобів захисту.

За допомогою SIEM можна домогтися майже абсолютної автоматизації процесу виявлення погроз. При коректному впровадженні такої системи підрозділ ІБ переходить на абсолютно новий рівень надання сервісу. SIEM дає змогу акцентувати увагу тільки на критичні та дійсно важливі загрози, працювати не з подіями, а з інцидентами, вчасно виявляти аномалії та ризики, запобігати фінансові втрати.

Важливо розуміти, що SEI – це інструмент не лише ІБ, але й взагалі ІТ. На основі потужних кореляційних механізмів можна ефективно забезпечувати безперервність роботи ІТ-сервісів, виявляти збої в роботі інформаційних і операційних систем, апаратного забезпечення. Крім того, SIEM – інструмент автоматизації. Найпростіший приклад, актуальний для більшості компаній: конфлікт IP-адрес. За рахунок найпростішого правила RBR можна довідатися про інцидент задовго до отримання скарги від користувача.

Аналіз реального використання SIEM на практиці показує, що в більшості випадків робота таких систем спрямована на консолідацію журналів подій від різних джерел. Фактично – використовується лише функціонал SI (Security Information). Якщо і є задані правила кореляції, вони не поповнюються.