Полотай О.І. к.т.н., доцент
Львівський державний університет безпеки життєдіяльності, Львів
Довганик С. студент
Національний університет «Львівська політехніка», Львів

SIEM-СИСТЕМИ, ЯК ЕЛЕМЕНТ АНАЛІЗУ ТА УПРАВЛІННЯ ПОДІЯМИ CSOC

Інформаційна система будь-якої, навіть найменшої компанії складна, і всі її частини повинні захищатися по одному і тому ж принципу - спочатку організаційні, потім превентивні заходи, потім засоби спостереження, які детектують аномалії, і інструменти реагування. Інструменти, які використовуються для захисту кожного з компонентів системи, можуть бути різними від компанії до компанії, але простежується загальна тенденція - поступово компанії, незалежно від їх розміру, приходять до ідеї впровадження CSOC – Cyber Security Operation Center. CSOC – це інфраструктура з безліччю взаємопов'язаних компонентів, його основа – SIEM (Security information and event management).

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.

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

Мета SIEM – аналіз інформації, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, тощо.

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.

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.***
- ***IDS / IPS-системи.***
- ***Антивірусні програми.***
- ***Журнали подій серверів і робочих станцій.***
- ***Міжмережеві екрани.*** Відомості про атаки, шкідливі програми та інше.
- ***Мережеве активне обладнання.***
- ***Сканери вразливостей.***
- ***Системи інвентаризації та asset-management.***
- ***Системи веб-фільтрації.***

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. Довганик С. Системи збору інформації про безпеку та управління подіями / Довганик С., Полотай О.І. // Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 року. Львів, ЛДУ БЖД, 2019, С. 7-9.