РОЗШИРЕННЯ ФУНКЦІОНАЛУ SIEM СИСТЕМ

Мінін Д.О., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: dmytro.minin@nure.ua.

Abstract. The subject of the study is undeclared capabilities of Security information and event management systems.

Багато компаній використовують SIEM-системи для виявлення інцидентів інформаційної безпеки різного ступеня складності і часто навіть не уявляють усі можливості власної системи моніторингу. Це пов'язано з тим, що співробітники відділу інформаційної безпеки часто не замислюються над додатковими функціями та можливостями, хоча ці знання могли б істотно допомогти в автоматизації цілого ряду процесів у відділі інформаційної безпеки (ІБ) або всієї компанії в цілому.

До основних таких недекларованих можливостей відносяться:

1) запуск зовнішніх скриптів та програм;

2) використання скорингової моделі;

3) застосування нейромереж для виявлення інцидентів ІБ.

Запуск зовнішніх скриптів і програм. Використовується, наприклад, для:

1) сканування хоста, у якому стався інцидент інформаційної безпеки;

2) запису в сторонні ресурси інформації про інцидент;

3) реалізація команд на віддаленій системі з метою виконання дій над користувачем або вузлом, що фігурує в інциденті ІБ.

Розглянемо докладніше перший сценарій – сканування хоста – і розглянемо ситуацію, при якій відбувається інцидент, пов'язаний зі спробами нелегітимних дій щодо очищення журналу аудиту та/або створення адміністративної групи на Linux-системі. При виявленні цієї події запускається скрипт збору з вузла додаткової інформації, пов'язаної з користувачем або групою. Результати роботи скрипта повертаються назад до SIEM-системи для фіксації всієї отриманої інформації про користувача або групи. Якщо інцидент призводить до його появи в системі управління інцидентами (Case Manager), то аналітику з ІБ буде набагато простіше прийняти рішення про критичність даного інциденту.

За такої реалізації робота вирішального правила про сканування хоста стає максимально продуктивною. Але варто враховувати той факт, що всі правила, які здійснюють запуски зовнішніх команд, повинні пройти етапи тестування та налагодження для мінімізації помилкових спрацьовувань та оптимізації завантаження системи. Для цього у SIEM-системі створюються механізми автоматичної перевірки коректності роботи правил та частоти їх спрацьовувань.

Використання скорингової моделі. Часто словосполучення "скорингова модель" асоціюється з антифрод-системами та боротьбою з фінансовими шахраями. Але реалізація скорингової моделі в інформаційній безпеці та SIEM-системі наразі є тією необхідністю, без якої повнота картини виявлення інцидентів ІБ не буде вичерпною.

Для використання складних кореляційних логік та виявлення складних ланцюжків інцидентів необхідно реалізовувати скорингову модель для підрахунку балів по кожному користувачеві та вузлу, що бере участь в інцидентах ІБ.

Так, наприклад, при спрацьовуванні правила Brute Force проводиться занесення до списку підрахунку скорингу як користувача, так і хоста, у якому відбувається спроба підбору пароля. При фіксації ряду інцидентів з користувачем або вузлом, що перебувають у аркуші скорингу, сумарний бал підвищується залежно від критичності інциденту. Таким чином, підсумовуючи бали за кожен інцидент, можна наочно оцінювати картину того, що відбувається, а також у разі реалізації додаткових механізмів можна контролювати інциденти, що відбуваються, і накладати на життєвий цикл кібератак Kill Chain з наступною класифікацією за MITRE.

Розглянемо наступний приклад. Створюється два списки (аркуші) з назвами User List та Host List:

– поля у User List – користувач, скоринг, дата;

– поля Host List – вузол, скоринг, дата.

Додаються до правил, що виявляють інциденти ІБ, дії щодо занесення користувача або хоста у відповідний лист, а також скорингове значення. Таким чином, у разі виявлення інцидентів у аркуші додається інформація про користувачів та хостів, що фігурують в інцидентах, а також підраховується скоринг по кожному користувачеві та хосту.

Такими діями можна створити додатковий механізм аналізу та можливості зміни критичності виявлення інцидентів, пов'язаних з тим чи іншим хостом або користувачем. У разі грамотно побудованої моделі можна активно реагувати на будь-які інциденти з ІБ.

Застосування нейромереж. Наразі все більший оборот набирає використання математичних моделей у сфері інформаційної безпеки, одним із прикладів яких є нейромережі.

Пропонується використовувати потужності SIEM-систем для генерації частини наборів даних для навчання нейромережі та мінімізації трудовитрат фахівців зі збирання та аналізу даних. Архітектура побудови інтеграції полягає в налаштуванні SIEM-системи в частині правил кореляції, мінімізації їх хибних спрацьовувань та подальшому вивантаженні кореляційних подій на набір даних (dataset) через шину даних. Для наочності розглянемо наступний приклад.

1. Треба навчити математичну модель для аналізу доменів третього рівня щодо наявності ряду артефактів, які можуть бути в запиті (наприклад

довжина доменного імені третього рівня понад 20 символів є підозрілою; не людино-читані слова в доменному імені є додатковою ознакою аномалії; фіксація доменного імені у репутаційних базах – ознака інциденту ІБ).

2. Здійснюється підключення DNS до SIEM та налаштування правил кореляції на виявлення довжини доменів третього рівня, у разі перевищення довжини запиту список доменів міститься в аркуші.

3. Аркуш відправляється на API лінгвістичного аналізу для отримання семантичного коефіцієнта розпізнання імені домену.

4. Як додатковий захід здійснюється надсилання запиту на платформу Threat Intelligence для аналізу доменного імені.

Таким чином, можна отримати багаторівневу систему аналізу доменних імен та складання списків "нормальних" та "ненормальних" імен для подальшого завантаження в набір даних (dataset).

Основна ідея цього прикладу полягає у демонстрації необхідності застосування автоматичних інтеграцій із сервісами, які можуть зменшити час підготовки набору даних для навчання моделі та заощадити ресурси фахівців DS/DM.

Зростання ефективності.

У докладі на конкретних прикладах було продемонстровано недекларовані можливості, що використовуються в SIEM-системах, і те, як вони дозволяють підвищити ефективність ситуаційного центру ІБ у цілому. Необхідність автоматизації процесів обробки інцидентів ІБ є одним із наріжних каменів у роботі будь-якого підрозділу захисту інформації. Щоб ефективно керувати системами моніторингу подій ІБ, необхідно перципувати (сприймати) і вміти використовувати весь спектр можливостей SIEM-систем.

Список використаних джерел.

1. Обзор решений SIEM (Security information and event management). Режим доступу: https://habr.com/ru/company/roi4cio/blog/528770/ (дата звернення 11.01.2022).

2. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Режим доступу: https://www.manaraa.com/Book/174707/security-information-and-event-management-(siem)-analysis-tr (дата звернення 11.01.2022).

3. Evaluation of Local Security Event Management System vs Standard Antivirus Software. Режим доступу: https://www.mdpi.com/2076-3417/12/3/1076/htm (дата звернення 11.01.2022).