УДК 004.056.53

ПРОПОЗИЦІЇ ЩОДО ВИКОРИСТАННЯ SPLUNK ДЛЯ АНАЛІЗУ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Вакуленко Д. В.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +380500002423

The purpose of this work is to study the automatic retrieval of logs from a Windows server machine and transfer them to the Splunk tool. And the automation of their analysis with the help of Python was also added

This work can be used during the automation of audit in Windows machines.

Відомо, що роботи з забезпечення кібербезпеки потрібно починати з аудиту систем. Щодня у всьому світі проводяться тисячі кібератак, які можуть призвести до втрати конфіденційної інформації. Все більше хакерів отримують доступ до систем до яких вони не повинні мати доступу. Дана тенденція свідчить про те, що довіряти певні дані інтернет сервісам є небезпечно.

З метою аудиту та аналізу функціонування інформаційних систем наразі створені системи, які аналізують лог-файли систем: SIEM/SOAR та їхні похідні.

SIEM/SOAR – «SIEM» називають злиття функцій управління інформацією про безпеку (SIM), тобто процес збору, моніторингу та аналізу даних з комп'ютерних журналів (звітів), які автоматично генеруються, та управління подіями безпеки (SEM) – процес централізації даних журналу комп'ютера з декількох джерел (систем, кінцевих точок, додатків і служб) для поліпшення виявлення інцидентів безпеки та управління цими подіями за допомогою формалізованого процесу реагування. Розвиток SIEM шляхом додавання автоматизації різних кейсів породило новий клас систем – SOAR. Залежно від того, що лежить в основі цієї системи, вона може мати різні назви: дії по забезпеченню безпеки, аналітика і звітність – Security Operations, Analytics and Reporting (SOAR) чи оркестрації подій безпеки та автоматичне реагування – Security Orchestration, and Automated Response. SOAR є спеціальним інструментом для узагальнення відомостей про загрози безпеки, які подаються з різних джерел, з подальшим аналізом цих даних [1].

У доповіді розглядається інформаційна система Splunk, яка може бути використана як SIEM (Security Information and Event Management), так і як SOAR (Security Orchestration, Automation and Response) [2 – 3].

Перевагами використання Splunk можна вважати:

– можливість збирати та аналізувати величезну кількість різноманітних даних із різних джерел, включаючи лог-файли, мережеві пристрої та бази даних;

– надання розширеної аналітики для виявлення патернів та аномалій, що допомагає забезпечити ефективніше виявлення атак та збільшити рівень безпеки.

Пропонується забезпечити ефективне використання Splunk у декілька етапів.

1. Налаштування Splunk на сервері, що являє собою програму, яка дозволяє збирати, зберігати та аналізувати різноманітні лог-файли з різних джерел та додатків. Задля збору даних, пропонується встановити додаток Universal Forwarder, що дозволить пересилати дані до апріорі налаштованого Splunk.

2. Написання Python скриптів, які дозволятимуть виконувати автоматизацію фільтрування даних, що були зібрані на попередніх етапах. Для цього в системі Splunk передбачений спеціальний дашбоард, який надає інформацію про успішне або не успішне виконання скриптів.

3. Перевірка налаштувань надання лог-файлів.

Отже, використання Splunk може бути спрямовано на підвищення ефективності збору та аналізу лог-файлів з ЕОМ з встановленою OS Windows. Враховуючи те, що зазначена система працює за допомогою мови програмування Python [4], що є мовою програмування для роботи з великими об’ємами даних, є можливість підвищення точності прийняття рішень, щодо виявлення вразливостей.

Відзначимо, що робота зі збору лог-файлів Windows-машин за допомогою Splunk дозволяє значно полегшити моніторинг подій, зменшити час, затрачуваний на аналіз та підвищити рівень безпеки інформаційної системи на підприємстві.

Список використаних джерел:

1. Що таке SIEM/SOAR. URL: https://amind.ua/systemy-upravlinnya-inform-bezpekoyu (дата звернення 11.04.2023)

2. Документація системи Splunk. URL: https://docs.splunk.com/Documentation/Splunk (дата звернення: 11.04.2023).

3. Splunk Universal Forwarder. URL: https://www.splunk.com/en_us/blog/learn/splunk-universal-forwarder.html (дата звернення 11.04.2023)

4. Integrate the Splunk platform using development tools for Python. URL: https://dev.splunk.com/enterprise/docs/devtools/python (дата звернення 11.04.2023)