УДК 004.056.2

ВИКОРИСТАННЯ SPLUNK ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ

Малькевич Р., Балацька В.
Львівський державний університет безпеки життєдіяльності, Львів

***Анотація**: Сучасне функціонування організацій будь яких форм власності практично неможливо без використання співробітниками різних серверів для роботи з даними, це безпосередньо впливає на рівень інформаційної безпеки. У роботі розглянуто використання інструменту Splunk, який функціонує на збиранні логів та виявлення в них подій.*

***Ключові слова**: Splunk, MapReduce, forwarder, big data, Splunk Enterprise Security.*

***Summary**: The modern functioning of organizations of any form of ownership is almost impossible without the use of employees of different servers to work with data, it directly affects the level of information security. The paper considers the use of the Splunk tool, which works on collecting logs and detecting events in them.*

***Keywords**: Splunk, MapReduce, forwarder, big data, Splunk Enterprise Security.*

Безпека та конфіденційність даних завжди були важливими, але враховуючи значні порушення, які відбулися протягом останніх двох років, вони стають все більш важливими з кожним днем. Для підвищення безпеки підприємств, організацій та захисту інформації у них, пропонується почати з більш ефективного використання даних, які система вже реєструє. Також для кращого захисту важливої інформації необхідно зібрати більше даних, щоб краще розуміти систему і легше помітити будь-які підозрілі події. У будь-якому випадку необхідно використовувати інструмент, який спеціалізується на роботі з даними журналів, щоб не доводилося читати неструктуровані дані з багатьох різних джерел. Ось тут на допомогу приходить Splunk.

Splunk – це система зберігання та аналізу логів [1]. Її принцип роботи можна описати так: є сервер Splunk, який зберігає, індексує та дозволяє аналізувати логи, і є робочі машини (сервери), які ці логи створюють і передають на сервер Splunk. Сервер Splunk в свою чергу може бути кластером з декількох фізичних машин, між якими розподіляється зберігання інформації і які використовуються для її обробки за технологією MapReduce. Способів передавати логи з робочих машин дуже багато: через спеціальну програму forwarder, яка вміє швидко і ефективно відсилати зміни логів на сервер, через технології типу NFS/SMB, або SNMP, можна самостійно відсилати дані в Splunk по TCP/IP (наприклад, замість того, щоб писати в файл). Під Windows Splunk вміє брати дані з Windows Events, Performance Counters або Реєстру.

Платформа Splunk фіксує та аналізує масивні шматки неструктурованих машинних даних. Запущений інструмент має можливість показати змістовне представлення даних, створених людиною [2]. DATA - нескінченна річ, у яку люди роблять свій внесок щодня. Розглянемо статистичні дані, які дадуть чітке уявлення про світ Big Data. Кількість користувачів мобільних мереж з кожним роком зростає, за останні 4-6 років кількість користувачів зросла на 1 мільярд. Мобільні телефони є основним джерелом більш ніж половини веб-трафіку у всьому світі. Одна з найпопулярніших пошукових систем є Googl обробляє більше 40 000 пошукових запитів щосекунди. І це лише Google, але окрім нього також існують інші пошукові системи, які теж оброблять величезну кількість запитів та інформації.

Як саме працює Splunk? [3]. Splunk має три основні фази роботи. У першій фазі, він ідентифікує дані за допомогою рішення. У другій фазі, ці машинні дані він перетворює в результати. І нарешті, у третій фазі, є змога конвертувати ці результати у звіти, діаграми або графіки для широкого використання візуальної інформації. Важливим компонентом є машинні дані, вони створюються та насичуються за допомогою нових технологій та систем, які люди використовують щодня. Одні з популярних сервісів є: AWS, APM, медичний простір, веб-сервери, системні журнали. Інформацію, яку поглинають дані сервіси, мають широке застосування та сприяють величезній кількості випадків використання у будь-якій з цих організацій. Самі дані є складними для розуміння масивами, що відображаються у різних форматах. Багато із традиційних інструментів або платформ не в змозі допомогти користувачам розібратись з цими даними і саме тут Splunk може голосно про себе заявити.

Splunk служить виявленням зловмисних дій співробітників та інших внутрішніх загроз до того, як станеться крадіжка конфіденційних даних, їх пошкодження чи зловживання повноваженнями [4]. За допомогою Splunk можна визначити неправильне використання дозволів, аномальну поведінку навіть у разі використання законних облікових записів, рівнів доступу або джерел. Наприклад, надмірно тривалі сеанси, нестандартний час або вхід. А дані, що накопичуються, про різні дії користувача дозволяють засновувати дослідження на історичних даних. У платформі можлива інтеграція з Active Directory або базами даних HR для отримання інформації про співробітників. Splunk дозволяє аналізувати інциденти для визначення обставин та масштабів інциденту. Це досягається за допомогою пошуку та знаходження кореляцій за ключовими словами, термінами або значеннями для різних мережевих пристроїв, хостів, зчитувачів і т.д. Для аналітиків безпеки це дає широкий контекст інциденту, що допомагає швидше та краще оцінювати рівень загрози, визначати причини та наслідки.

Також архітектури безпеки зазвичай включають різні рівні інструментів і продуктів. Як правило, вони не призначені для спільної роботи та

містять прогалини у питаннях роботи фахівців з безпеки щодо встановлення зв'язків між різними доменами. Splunk усуває ці прогалини, забезпечуючи єдиний інтерфейс для автоматичного вилучення даних, що дозволяє будувати комплексну аналітику та реагувати на погрози серед продуктів різних постачальників.

Основним прикладом готових рішень є Splunk Enterprise Security (ES) [5] — система управління інформаційною безпекою та подіями (англ. Security and information event management, SIEM), яка формує докладну картину машинних даних, що створюються різними технологіями безпеки (мережа, кінцеві точки, доступ, шкідливі програми, вразливість). Завдяки Splunk Enterprise Security фахівці з безпеки можуть швидко виявляти внутрішні та зовнішні атаки та вживати заходів у відповідь. Це дозволяє спростити операції із захисту від загроз, мінімізувати ризик та забезпечити безпеку бізнесу. Splunk Enterprise Security оптимізує всі аспекти захисту та підходить для організацій будь-якого масштабу та професійного рівня. Організації по всьому світу використовують Splunk Enterprise Security (ES) як SIEM для моніторингу безпеки, розширеного виявлення загроз, реагування на інциденти та використання широкого спектру аналітичних програм для аналізу безпеки.

Висновок: незалежно від того, у якій галузі функціонує підприємство, воно створює величезну кількість даних , що генеруються веб-сайтами, додатками, серверами, мережевими та мобільними пристроями. Це одна з найбільш швидко зростаючих і складних частин великих даних. Програмне забезпечення Splunk перетворює зібрану інформацію у цінні дані в режимі реального часу. Ці відомості поглиблюють розуміння клієнта, покращують рівень обслуговування, знижують експлуатаційні витрати та зменшують ризики кібербезпеки.

Література

1. Splunk для аналізу логів [Електронний ресурс] – Режим доступу: https://www.mogroup.com.ua/?p=205, вільний;

2. Splunk [Електронний ресурс] – Режим доступу: https://techexpert.ua/it-products/splunk-platform/, вільний;

3. What's new at Splunk [Електронний ресурс] – Режим доступу: https://www.splunk.com/, вільний;

4. Splunk® [Електронний ресурс] – Режим доступу: https://auditagency.com.ua/splunk/, вільний;

5. Security Information and Event Management (SIEM) with Splunk [Електронний ресурс] – Режим доступу: https://www.cprime.com/resources/blog/security-information-and-event-management-siem-splunk/, вільний.